CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

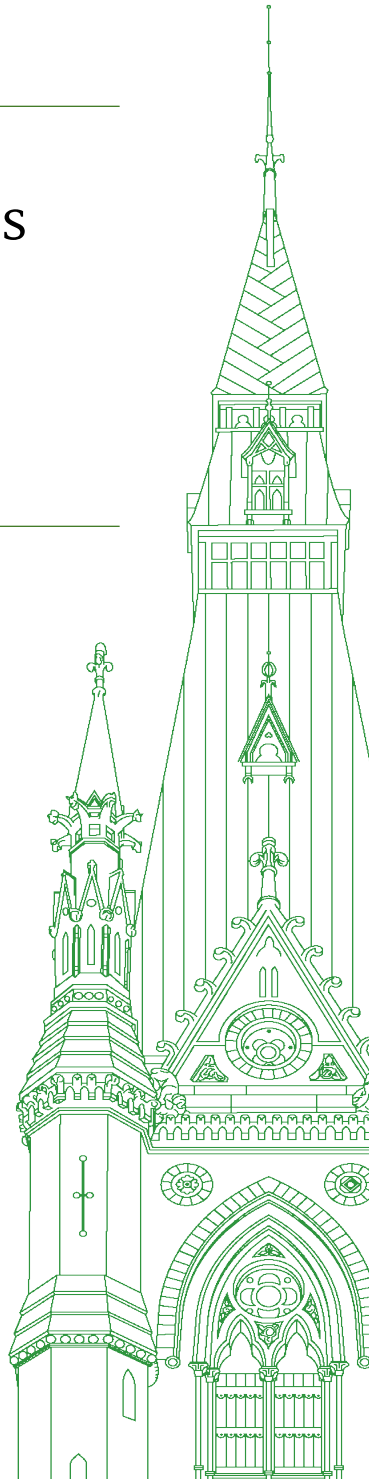
43e LÉGISLATURE, 1re SESSION

Comité permanent des opérations gouvernementales et des prévisions budgétaires

TÉMOIGNAGES

NUMÉRO 014

Le lundi 25 mai 2020



Président : M. Tom Lukiwski

Comité permanent des opérations gouvernementales et des prévisions budgétaires

Le lundi 25 mai 2020

● (1700)

[*Traduction*]

Le président (M. Tom Lukiwski (Moose Jaw—Lake Centre—Lanigan, PCC)): La séance est ouverte.

Je vous souhaite la bienvenue, chers collègues, à la 14e réunion du Comité permanent des opérations gouvernementales et des prévisions budgétaires.

Notre créneau horaire est de 17 à 19 heures, mais la ministre ne peut rester avec nous que pendant la première heure. En revanche, ses collaborateurs resteront jusqu'à 19 heures.

La prochaine réunion du Comité aura lieu vendredi, de 11 à 13 heures, heure normale de l'Est. Les whips ne nous ont pas encore informés de nos dates de réunions pour la semaine prochaine. Dès que nous aurons ces informations, nous les transmettrons directement à tous les membres du Comité.

Permettez-moi de faire plusieurs rappels concernant la procédure et le déroulement de nos travaux.

Nous procéderons aux trois séries de questions sur lesquels nous nous sommes entendus, la première de six minutes, la deuxième de cinq minutes et la troisième de deux minutes et demie, ce qui nous permettra de poser un maximum de questions. La ministre Murray doit absolument nous quitter à 18 heures, mais les témoins resteront et nous passerons alors à la deuxième série de questions.

Je vous demande de ne pas alterner entre le français et l'anglais quand vous faites une déclaration ou que vous posez une question, car cela nous a posé des difficultés techniques dans le passé. Je vous invite donc à ne pas le faire, cela facilitera le bon déroulement de notre réunion et nous évitera de perdre du temps parce que les techniciens auront dû interrompre nos délibérations.

Cela dit, chers collègues, vous savez tous comment procéder.

Madame la ministre, je suis ravi de vous revoir. Vous avez une déclaration liminaire de cinq minutes, je crois.

Madame la ministre, vous avez la parole.

L'hon. Joyce Murray (ministre du Gouvernement numérique): Merci beaucoup, monsieur le président. C'est bon de revoir tout le monde en séance virtuelle.

Je suis ravie de comparaître devant votre comité depuis mon domicile, qui est situé sur le territoire traditionnel des Salish de la Côte. Je suis accompagnée aujourd'hui de M. Paul Glover, président de Services partagés Canada; de M. Raj Thuppal, sous-ministre adjoint principal des réseaux, de la sécurité et des services numériques; de M. Marc Brouillard, dirigeant principal de l'information du Canada par intérim; et de M. Scott Jones, dirigeant principal du Centre canadien pour la cybersécurité.

Monsieur le président, chers collègues, en qualité de ministre du Gouvernement numérique, c'est moi qui pilote, au sein du gouvernement canadien, le dossier de la transformation numérique. Mon mandat consiste à donner aux fonctionnaires les outils dont ils ont besoin et de mettre en place les services numériques auxquels les Canadiens s'attendent. Cette transformation est absolument cruciale si le gouvernement veut rester en phase avec l'évolution des techniques numériques, et, comme l'a montré la pandémie, il est plus important que jamais d'avoir des services numériques sécurisés, fiables et faciles à utiliser, afin qu'aucun Canadien ne soit laissé pour compte.

Il y a une dizaine de semaines, notre gouvernement a pris la décision inédite de demander aux employés fédéraux de faire du télétravail à partir de chez eux, et conséquemment, dans tous les ministères, nos équipes numériques ont dû redoubler d'efforts pour s'assurer que les fonctionnaires pouvaient continuer de travailler efficacement et en toute sécurité, car la première priorité de notre gouvernement est de continuer de servir les Canadiens.

J'ai été très impressionnée par les efforts déployés par Services partagés Canada, le Bureau du dirigeant principal de l'information et le Service numérique canadien pour accroître nos capacités numériques quasiment du jour au lendemain. Services partagés Canada veille à la prestation efficace et sécurisée des services numériques essentiels dont les citoyens ont de plus en plus besoin, en plus d'assurer un appui informatique auprès des fonctionnaires qui sont en télétravail et qui n'ont jamais été aussi nombreux à le faire. C'est un travail colossal, et je remercie tous les fonctionnaires qui contribuent à sa réalisation.

Services partagés Canada a développé les réseaux, renforcé les services et fourni des équipements et des outils aux employés en télétravail pour que ceux-ci puissent continuer de fournir des services essentiels à la population. Ils ont aussi fait en sorte que les employés puissent faire et recevoir des appels en Wi-Fi, lorsque la couverture cellulaire est insuffisante, et ils ont augmenté la capacité Internet des ministères, parfois jusqu'à 300 %. Ils ont quasiment doublé la capacité d'accès sécurisé à distance du gouvernement, de sorte que nous pouvons maintenant utiliser jusqu'à 270 000 connexions à distance en même temps. Services partagés Canada a également triplé la capacité de l'Agence du revenu du Canada afin de lui permettre de gérer l'avalanche de demandes pour la Prestation canadienne d'urgence et la Prestation canadienne d'urgence pour les étudiants.

Le Service numérique canadien a également mis au point des solutions numériques pour l'ensemble des ministères, notamment une boîte à outils numériques pour aider les ministères à recruter des techniciens et à utiliser une bibliothèque de solutions à code source ouvert, et pour aider aussi les citoyens à naviguer parmi les multiples prestations disponibles et à s'inscrire pour recevoir les avis de Santé Canada et d'autres ministères en ce qui concerne la COVID-19.

Le Bureau du dirigeant principal de l'information fournit à tous les ministères des conseils informatiques pour les services liés à la COVID-19, et il s'assure que les offres du secteur privé sont évaluées et mises en œuvre rapidement de concert avec les ministères. Dans le but de protéger les informations, ce bureau a aidé tous les fonctionnaires fédéraux à sécuriser leur système de télétravail et à utiliser les outils numériques en toute sécurité.

Toute crise attire les pirates informatiques, et nous restons très vigilants, car l'utilisation croissante de nouveaux outils numériques s'accompagne d'un risque accru de cyber activités malveillantes. La cybersécurité continue d'être une priorité absolue du gouvernement, et nous nous employons à protéger les Canadiens contre les cybermenaces. Je peux vous assurer que nous surveillons en permanence toute cybermenace éventuelle, afin de la neutraliser, et que nous coordonnons efficacement ce type d'activités grâce au Plan de gestion des événements de cybersécurité du gouvernement du Canada.

Services partagés Canada a augmenté la sécurité globale du gouvernement en implantant des services comme la défense périphérique, la gestion des vulnérabilités, l'intégrité de la chaîne d'approvisionnement et un programme de sécurité informatique et de cybersécurité intégrée pour protéger les infrastructures qui desservent les départements et agences.

Pour lutter contre les fausses informations sur la COVID-19, le Centre canadien pour la cybersécurité a collaboré avec des partenaires de l'industrie et a supprimé des milliers de sites Web frauduleux et d'adresses de courriel susceptibles de servir à des activités malveillantes.

● (1705)

En conclusion, je voudrais dire que toute crise peut être une occasion d'améliorer les choses, et c'est le cas avec cette pandémie. Très rapidement, un élan de collaboration s'est instauré dans tous les paliers de gouvernement et dans l'industrie. Nous avons mis en place des solutions numériques qui nous ont permis de relever des défis inouïs à une vitesse inouïe, et ce, en toute sécurité. Je remercie tous nos fonctionnaires qui ont participé à cet effort technologique qui représentait une tâche herculéenne.

Je vous remercie. Je suis maintenant disposée à répondre à vos questions.

Le président: Merci beaucoup.

Je donne la parole à M. Aboultaif, pour six minutes.

M. Ziad Aboultaif (Edmonton Manning, PCC): Bonjour, madame la ministre. J'espère que vous et votre famille êtes en bonne santé.

J'ai entendu dire que des centaines de milliers d'informations confidentielles avaient été piratées chez Zoom. J'ai aussi entendu parler d'un cas semblable chez Skype, où des vidéos auraient été volées à l'insu des utilisateurs.

Nous utilisons Zoom et parfois aussi d'autres logiciels comme Skype. Lorsque nous sommes en discussion en vidéo, est-ce que les informations sensibles dont nous disposons sont bien protégées contre un piratage? Est-ce que nous prenons toutes les mesures pour que ces informations ne tombent pas entre de mauvaises mains?

L'hon. Joyce Murray: Premièrement, nous savons que, pendant une pandémie, il y en a toujours qui cherchent à profiter de la crise, et nous prenons toutes les précautions pour nous assurer que les Canadiens et nos systèmes sont protégés.

Vous avez parlé de Zoom. Je crois savoir que la Chambre des communes utilise Zoom pour le Parlement virtuel. Tout le monde sait que ce n'est pas une application sécurisée, et on ne l'utilise pas dans la fonction publique ni au Parlement lorsque les informations doivent rester confidentielles. Zoom et les autres outils publics ne peuvent être utilisés que pour des discussions et des informations publiques.

Nous donnons des conseils aux fonctionnaires en ce qui concerne les outils appropriés à utiliser pour tel ou tel service fourni aux Canadiens.

M. Ziad Aboultaif: Madame la ministre, un grand nombre de fonctionnaires font du télétravail, aussi bien des politiciens que n'importe qui d'autre. Plusieurs ministères sont administrés à distance, par des télétravailleurs qui s'échangent des informations sensibles.

Savez-vous si des informations sensibles ont fait l'objet de fuites, avez-vous reçu des plaintes à ce sujet?

L'hon. Joyce Murray: Monsieur Aboultaif, je vais demander à mes collaborateurs de compléter ma réponse parce qu'ils ont plus de détails là-dessus, mais personnellement, je n'ai entendu parler d'aucune intrusion dans nos systèmes.

Nous avons rapidement augmenté la capacité des réseaux sécurisés pour qu'ils puissent desservir les fonctionnaires en télétravail. En fait, avant la pandémie, il y avait chaque jour, à un point donné, une moyenne d'environ 40 000 connexions sécurisées à distance. Aujourd'hui, il y en a 200 000, ce qui signifie que nos réseaux sécurisés ont pu s'adapter très rapidement aux besoins des fonctionnaires en télétravail. Nous avons également créé des réseaux sécurisés nuage-sol pour certains autres types d'activités.

C'est une question importante, et je pense que les fonctionnaires réussissent à protéger l'intégrité...

● (1710)

M. Ziad Aboultaif: Madame la ministre, avez-vous évalué le niveau de sécurité de Zoom avant qu'on ne commence à l'utiliser, et depuis quand cette application est-elle utilisée au gouvernement, par qui que ce soit?

L'hon. Joyce Murray: Ma réponse est oui. Zoom est utilisé par des fonctionnaires, mais uniquement lorsque leurs communications sont publiques ou peuvent être rendues publiques. Mais lorsqu'il s'agit d'informations confidentielles ou à diffusion restreinte, Zoom ne peut pas être utilisé. Le dirigeant principal de l'information a énoncé des directives très claires là-dessus. Je vais maintenant donner la parole à mes collaborateurs, s'ils ont quelque chose à ajouter.

Je sais que dans ce format, c'est un peu plus difficile, mais s'ils ont quelque chose à ajouter, je les invite à le faire.

Monsieur Glover.

M. Paul Glover (président, Services partagés Canada): Merci, madame la ministre.

Nous avons bien sûr procédé à une évaluation du niveau de sécurité de tous les logiciels, afin de nous assurer que nous pouvions les utiliser. C'est ce qu'indiquent les directives dont la ministre a parlé et que le dirigeant principal de l'information a communiquées à tous les ministères.

Nous avons donné aux ministères un accès à distance sécurisé afin que leurs employés en télétravail puissent en profiter. Au début, comme il n'y avait pas assez de bande passante et de connexions à distance sécurisées, nous avons aussi mis à leur disposition des canaux non sécurisés afin de réserver les canaux sécurisés aux informations sensibles. C'est ce que nous continuons de faire.

M. Ziad Aboultaif: J'ai une petite question.

Il y a manifestement eu quelques intrusions dans nos systèmes, si j'ai bien compris le collaborateur de la ministre, et je vais vérifier. Avez-vous eu échangé des renseignements avec d'autres partenaires comme le Groupe des cinq, sur des incidents qui se seraient produits chez nous ou ailleurs chez nos alliés?

Le président: Soyez brève, je vous prie.

L'hon. Joyce Murray: Nous exerçons une surveillance constante, et, en effet, le Centre canadien pour la cybersécurité, dont mon ministère est partenaire, travaille en étroite collaboration avec le Groupe des cinq afin de détecter les menaces.

Le président: Merci beaucoup.

Je donne maintenant la parole à M. MacKinnon, pour six minutes.

[*Français*]

M. Steven MacKinnon (Gatineau, Lib.): Je vous remercie, monsieur le président.

Je suis ravi de voir ma collègue la ministre et les gens qui l'accompagnent aujourd'hui.

Pour être passé par Services partagés Canada, je suis extrêmement fier de tout ce que ces gens ont réussi à mettre en œuvre sur le plan des ressources. Les progrès que nous constatons à Services partagés Canada sont assez remarquables. Alors, madame la ministre, je tiens à souligner le succès des hommes et des femmes de Services partagés Canada qui ont fourni aux fonctionnaires l'accès aux réseaux sécurisés et aux outils technologiques dont ils avaient besoin pour maintenir les services offerts aux citoyens pendant cette crise. Je sais que Services partagés Canada a souvent été la cible de critiques, mais cette fois, elle nous montre la voie à suivre. Nous sommes très fiers de ce que ces gens ont pu accomplir.

[*Traduction*]

Je sais que mes collègues n'apprécient pas toujours que nous parlions ici de ce qui marche bien, madame la ministre, mais je pense qu'il est important qu'on reconnaisse le travail incroyable qu'accomplissent les hommes et les femmes qui composent notre fonction publique.

On dit de plus en plus que tout le monde va pouvoir faire du télétravail, que les centres-villes vont se vider et que personne ne sera plus jamais obligé de se rendre à son bureau.

Madame la ministre, vous travaillez beaucoup sur tout ce qui concerne la technologie en milieu de travail. Services publics et Approvisionnement Canada s'y intéresse aussi beaucoup, dans le but de permettre une plus grande flexibilité, des bureaux non dédiés et des lieux de travail mieux adaptés au futur, et ce, en partie grâce aux technologies. Où en est votre réflexion à ce sujet?

L'hon. Joyce Murray: Merci, monsieur MacKinnon.

On a bien sûr beaucoup parlé dans les médias de la crise à laquelle nous avons dû répondre en augmentant considérablement nos outils numériques sécurisés et des répercussions que cela aura sur la période d'après-COVID-19. Nous réfléchissons sérieusement à la stratégie que nous devrons alors mettre en place.

Je pense que nous avons tous été surpris, agréablement surpris je dirai, par la rapidité avec laquelle le gouvernement a réussi à s'adapter pour continuer à servir les Canadiens et même à améliorer la qualité du service. Comme vous le savez, près d'un million de Canadiens ont fait une demande pour la PCU dès le premier jour.

Je pense que c'est une évolution qui se poursuit depuis un certain temps déjà. Le budget de 2018 a débloqué plus de 2 milliards de dollars sur cinq ans pour favoriser une approche plus intégrée en ce qui concerne l'entreposage des données et le gouvernement numérique. C'était le budget de Services partagés Canada. Là-dessus, un demi-milliard de dollars ont été consacrés à la cybersécurité et à la mise en place d'une approche concertée dans ce domaine, ce qui nous est particulièrement utile en ce moment. S'agissant des vieux centres de données et de leur migration, je pense qu'environ 40 % d'entre eux ont été transférés dans des centres modernes et dans le nuage.

Notre gouvernement s'est particulièrement intéressé à des aspects importants qui n'avaient peut-être pas reçu toute l'attention nécessaire au fil des ans, et c'est précisément ce à quoi s'emploie le ministère du Gouvernement numérique, dans l'objectif de mieux servir les Canadiens. En matière de prestation de services publics, on ne peut pas offrir aux Canadiens que des solutions qui obligent les citoyens à télécharger des PDF, à télécopier des documents ou à faire la queue devant un guichet.

● (1715)

M. Steven MacKinnon: Nous sommes dans un nouveau monde.

Je sais que le président va bientôt m'interrompre, mais je voudrais simplement faire remarquer ou même demander… Nous avons consacré beaucoup de temps à la mise en place de services de base comme le Wi-Fi dans le nouveau poste de travail standard des fonctionnaires fédéraux, pour leur permettre de communiquer d'un ministère à l'autre dans un environnement moderne, plus propice à la créativité. Tout ça va être intégré dans le milieu de travail. Pourriez-vous nous dire ce que vous en pensez, s'il nous reste du temps?

Le président: Malheureusement, il ne vous reste plus de temps.

M. Steven MacKinnon: Très bien.

Le président: Si vous voulez répondre à la question de M. McKinnon, madame la ministre, je vous invite à le faire par écrit le plus rapidement possible et à envoyer votre réponse à notre greffier.

L'hon. Joyce Murray: Parfait.

[*Français*]

Le président: Madame Vignola, vous avez la parole pour six minutes.

Mme Julie Vignola (Beauport—Limoilou, BQ): Je vous remercie, monsieur le président.

Bonjour, madame Murray.

En effet, le virage que les employés ont pris au cours des derniers mois est spectaculaire. Il n'en demeure pas moins que nous aurons beaucoup de questions à cet égard.

Le 8 mai dernier, le dirigeant principal de l'information par intérim a dit au Comité qu'il y avait une surveillance continue du réseau du gouvernement fédéral de la part du Centre de la sécurité des télécommunications.

Quels sont les plus grands risques, les principales menaces, pour le réseau du gouvernement fédéral? Comment le gouvernement fédéral atténue-t-il ces risques et ces menaces?

[*Traduction*]

L'hon. Joyce Murray: Je vous remercie de votre question, madame Vignola.

L'important, je pense, c'est que nous ayons une approche intégrée face aux menaces. À une époque, chaque ministère devait se débrouiller tout seul. Aujourd'hui, nous avons une approche très intégrée, par l'intermédiaire du Centre canadien pour la cybersécurité.

Le système marche bien, à preuve, la mise en place des nouvelles prestations d'urgence, qui s'est faite très rapidement. Des experts en cybersécurité surveillent en permanence cette application afin de s'assurer qu'il n'y a pas de vulnérabilités et qu'aucune attaque ne perturbe notre service.

C'est une approche fondée sur la concertation. Chaque ministère a une responsabilité claire et distincte en ce qui concerne la prévention des menaces et des attaques de cybersécurité et les mesures à prendre. C'est un système qui marche très bien.

● (1720)

[*Français*]

Mme Julie Vignola: Dans votre allocution, vous faisiez référence aux sites Web frauduleux qui copiaient les sites du gouvernement du Canada. Combien de ces sites Web ont été détectés? Ont-ils tous été mis hors d'état de nuire?

[*Traduction*]

L'hon. Joyce Murray: Je vais demander au représentant du Centre canadien pour la cybersécurité, Scott Jones, de vous donner plus de détails.

Je dois dire que, grâce à la surveillance du système et à la mise en place d'un périmètre très efficace dans lequel sont confinées toutes les activités sécurisées du gouvernement, nous n'avons pas enregistré de cyberincidents sérieux depuis le début de la pandémie, alors que le nombre d'activités a fortement augmenté.

Scott, avez-vous quelque chose à ajouter?

M. Scott Jones (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Oui. Merci, madame la ministre.

En général, nous travaillons avec nos partenaires commerciaux et les centres de cybersécurité partout dans le monde pour détecter tout site cherchant à se faire passer pour le gouvernement du Canada afin de tromper les Canadiens et de les amener à faire certaines choses en ligne. Nous avons fermé des centaines de sites Web et d'indicateurs malveillants, et nous avons aussi montré au secteur commercial à quoi ressemblait le site officiel de la PCU, pour qu'ils puissent le reconnaître et fermer eux aussi les sites malveillants. De cette façon, nous protégeons rapidement tous les Canadiens.

[*Français*]

Mme Julie Vignola: Pourriez-vous nous dire combien il y a eu de victimes avant que ces sites soient détectés par vos services?

[*Traduction*]

M. Scott Jones: Malheureusement, comme nous sommes à l'affût des activités malveillantes, nous ne surveillons pas les Canadiens. La Loi sur le CST nous interdit de surveiller les Canadiens. Nous ne savons donc pas combien il y a de victimes. Nous devons nous adresser à nos collègues du Centre antifraude du Canada pour savoir si un Canadien a signalé le problème.

[*Français*]

Mme Julie Vignola: Y a-t-il des employés de la fonction publique faisant du télétravail dont le système informatique a été ciblé par une cyberattaque?

[*Traduction*]

M. Scott Jones: En général, le gouvernement du Canada est la cible d'environ deux milliards d'activités malveillantes par jour. De ce nombre, il y en a beaucoup qui sont simplement des activités de reconnaissance pour repérer des services vulnérables, mais nous sommes en mesure d'intervenir et de bloquer ces activités-là avec nos collègues de Services partagés Canada.

Eh oui, les utilisateurs des sites du gouvernement du Canada sont aussi ciblés. La très grande majorité de ces tentatives, plus de 99 %, sont bloquées avant que le fonctionnaire ne s'en rende compte.

[*Français*]

Mme Julie Vignola: Parmi le 1 % des cyberattaques qui reste, y a-t-il eu des conséquences soit sur les données gouvernementales, soit sur les données personnelles des Québécois et des Canadiens?

[*Traduction*]

Le président: Soyez très bref, monsieur Jones, s'il vous plaît.

M. Scott Jones: Aucun système gouvernemental n'a fait l'objet d'une intrusion depuis le début de la crise.

Le président: Merci beaucoup.

Je donne maintenant la parole à M. Green, pour six minutes.

M. Matthew Green (Hamilton-Centre, NPD): Merci beaucoup, monsieur le président.

Je suis ravi que la ministre participe à notre réunion aujourd'hui.

Comme vous le savez, les bureaux de circonscription au Canada ont été inondés d'appels chaque fois que le gouvernement faisait une nouvelle annonce, surtout en ce qui concerne les prestations d'assurance-emploi et la PCU, et c'est sans doute la même chose pour les petites entreprises, par conséquent, j'imagine que vous avez dû accomplir une tâche herculéenne pour que les différents services gouvernementaux puisent répondre à ces demandes.

Pour autant, de nombreuses personnes nous ont dit avoir eu des problèmes en ce qui concerne le traitement de leur demande d'assurance-emploi ou de PCU, et ne pas avoir pu parler à un agent de l'Agence du revenu ou de Service Canada. Une électrice de ma circonscription, Mme Shannon Cooper, a fait une demande pour un congé d'assurance-emploi le 19 mars dernier, et elle attend toujours de recevoir son premier paiement. Elle a dû appeler Service Canada pour régler toutes sortes de problèmes concernant sa demande. Trop souvent, lorsqu'elle réussissait finalement à avoir un agent au téléphone, l'appel était coupé et l'agent ne la rappelait pas. Ça lui est arrivé maintes et maintes fois. Aujourd'hui, elle en est presque à 70 jours sans salaire.

Parmi toutes les difficultés informatiques que connaissent certainement tous les ministères du gouvernement, êtes-vous au courant que les centres d'appels coupent les appels avec les Canadiens?

● (1725)

L'hon. Joyce Murray: Vous savez...

Le président: Madame la ministre, avant de vous laisser répondre, je voudrais simplement rappeler encore une fois à M. Green qu'il doit limiter ses questions à la réponse du gouvernement à la pandémie de la COVID-19. C'est le cadre de notre mandat.

M. Matthew Green: Monsieur le président, j'estime, avec tout le respect que je vous dois, que les demandes de PCU s'inscrivent tout à fait dans le cadre de la COVID-19 et que c'est une question importante.

Le président: C'est une question importante, certes, mais je veux simplement m'assurer que la question est bien ciblée.

Vous avez la parole.

M. Matthew Green: Oui, elle porte à 100 % sur la PCU.

L'hon. Joyce Murray: Je vous remercie de votre question.

Il est bien évident que l'objectif prioritaire de notre gouvernement est de servir les Canadiens de façon rapide, efficace et sécurisée, et c'est donc toujours avec regret que j'apprends que quelqu'un a des difficultés à contacter un agent du gouvernement.

Je dois dire que, malgré les efforts des fonctionnaires canadiens pour s'adapter au télétravail et des employés des centres d'appels qui sont eux aussi, parfois, en télétravail, la situation a été assez difficile. Des millions de Canadiens ont demandé l'aide du gouvernement et des millions de Canadiens l'ont reçue, ce dont je suis très fière, mais nous ne cessons jamais d'améliorer nos systèmes, nos infrastructures et les outils sécurisés dont nous avons besoin.

M. Matthew Green: C'est la réponse que j'attendais, de la part du gouvernement. Toutefois, si on veut trouver une solution aux difficultés qui se posent, et qui concernent peut-être davantage l'ancienne technologie — vous voudrez peut-être revenir là-dessus tout à l'heure —, savez-vous exactement quel pourcentage d'appels sont coupés? Sur quelles données vous fondez-vous pour essayer d'améliorer les systèmes informatiques?

L'hon. Joyce Murray: Je vous remercie de votre question. Je vais demander à M. Paul Glover d'y répondre.

M. Paul Glover: Merci, madame la ministre, et merci à vous, monsieur le président, de me permettre de répondre à la question du député.

Nous sommes parfaitement au courant de ces problèmes, et j'ai le plaisir de vous informer que la situation s'améliore de jour en jour. Le nombre d'appels adressés par des Canadiens à EDSC et à l'ARC a atteint des records, si bien que des mesures ont été prises pour améliorer la capacité du système et acheminer rapidement les appels vers les agents appropriés.

Quant au nombre d'appels coupés, nous avons fait des vérifications et amélioré les systèmes en conséquence, de sorte qu'aujourd'hui, il n'y en a presque plus.

M. Matthew Green: J'aime bien les généralités, mais je préfère avoir des chiffres précis...

M. Paul Glover: Hier, il n'y en a pas eu un seul.

M. Matthew Green: Pas un seul. Aucun appel n'a été coupé hier. C'est ce que vous affirmez?

M. Paul Glover: Bien sûr, tout dépend de ce que vous entendez par « coupé ». Quand la ligne est occupée, parce qu'il y a une limite au nombre d'appels passant par cette ligne ou parce que le système sait qu'il doit mettre l'appelant en attente compte tenu de la durée moyenne des appels précédents, la personne entend le signal que la ligne est occupée et sait qu'elle ne peut même pas être placée en attente. Si on ne tient pas compte de ces appels, aucun de tous les autres qui sont entrés en ligne et qui ont été acheminés à un agent n'a été coupé au cours des derniers jours.

M. Matthew Green: Pour en terminer avec cette question, je suis très content d'apprendre qu'il y a eu des améliorations. Je crains cependant que nos bureaux de circonscription ne partagent pas cet avis.

Depuis le début de cette vague sans précédent d'appels coupés et jusqu'à aujourd'hui, quel a été le nombre record d'appels coupés, en avez-vous une idée?

M. Paul Glover: Nous transmettrons ces informations au greffier, je préfère éviter de donner des chiffres approximatifs.

Je sais qu'un certain nombre de mesures ont été prises. Dans certains cas, les appels n'étaient pas coupés, mais la personne n'obtenait pas de réponse, tout simplement. C'est un autre problème. L'appel passe, mais il n'est pas coupé parce que personne ne répond. Les ministères ont pratiquement doublé le nombre d'agents pour répondre à ces appels, donc le problème devrait être réglé.

En plus d'avoir réglé le problème des appels coupés, nous avons essayé d'augmenter le nombre de lignes pour que les gens puissent utiliser le répondeur vocal. Ils peuvent continuer à appeler, mais au lieu de parler à un agent, ils choisissent une question dans la foire aux questions, ils entrent leurs informations s'ils n'ont pas accès à un ordinateur et ils peuvent ainsi faire leur demande de prestation. Nous avons augmenté le nombre de lignes, et ça a amélioré les choses.

Nous vous ferons parvenir une liste de toutes les mesures que nous avons prises jusqu'à aujourd'hui.

● (1730)

M. Matthew Green: Ce sera utile.

Monsieur le président, merci beaucoup.

Le président: Merci beaucoup.

Nous allons maintenant entamer la série de questions de cinq minutes, et commencer encore une fois par M. Aboultaif.

M. Ziad Aboultaif: Merci, monsieur le président.

Madame la ministre, le gouvernement fédéral veut aider les provinces à construire un dispositif qui permet le traçage des contacts au moyen d'un appareil cellulaire personnel. Est-ce que cette initiative est antérieure à la pandémie?

L'hon. Joyce Murray: Il serait préférable de poser la question à la ministre de la Santé, mais je vais essayer de vous donner une réponse.

Je crois que cette initiative s'inscrit dans le cadre de notre réponse à la pandémie, avec comme objectif de relancer notre économie et de permettre à nos entreprises de continuer à servir les Canadiens. Pour l'instant, il faut faire davantage de traçage des contacts et plus de tests, et comme cela relève de la responsabilité des provinces, le gouvernement fédéral leur a offert son aide.

M. Ziad Aboultaif: À ce propos, nous savons que le gouvernement a déjà essayé, dans le passé, de porter atteinte à la vie privée des Canadiens, notamment lors de l'affaire de Statistique Canada et des informations bancaires personnelles, lorsque 500 000 dossiers environ ont été divulgués à l'insu des Canadiens.

Nous savons que les Canadiens sont très inquiets lorsque l'on porte atteinte à leur vie privée et qu'on divulgue des informations personnelles. Et cela s'ajoute au fait, bien évidemment, qu'ils sont sous surveillance constante. Ils sont sous surveillance en permanence.

Est-il possible, oui ou non, que cette initiative de traçage des contacts, qui est facultative pour le moment, devienne un jour obligatoire?

L'hon. Joyce Murray: Je ne peux pas vous répondre, tout ce que je peux dire...

M. Ziad Aboultaif: Madame la ministre, je comprends, mais il s'agit quand même de votre ministère car, au final, c'est lui qui va faire le travail.

L'hon. Joyce Murray: Je sais que nous allons fournir des conseils, des recommandations et du soutien, en tant que ministère du Gouvernement numérique, mais ce sont les provinces qui sont responsables des tests et du traçage. Le gouvernement fédéral leur a offert une aide financière pour leur permettre de faire davantage de tests ainsi que des ressources humaines pour faire le traçage des contacts. Par l'entremise du dirigeant principal de l'information et de nos autres fonctionnaires, nous appliquons des politiques et des lignes directrices très strictes sur le respect de la vie privée des Canadiens.

M. Ziad Aboultaif: Autrement dit, vous ne vous contentez pas d'une aide financière, vous leur donnez également des lignes directrices ou des conseils quant à la façon de procéder.

C'est très important parce que les Canadiens s'intéressent à deux choses: le respect de leur vie privée, d'une part, et les renseignements dont le gouvernement a besoin, d'autre part.

Comment allez-vous trouver un juste équilibre entre la sécurité publique et le respect de la vie privée?

L'hon. Joyce Murray: S'agissant du respect de la vie privée, nous avons des lignes directrices et des lois qui s'appliquent. Par exemple, Services partagés Canada a pris l'initiative de dresser une liste des choses à faire pour respecter la vie privée et pour mesurer l'impact sur la vie privée.

Lorsqu'il veut collecter, utiliser et divulguer des données à d'autres fins que celles pour lesquelles il les a collectées au départ, le gouvernement doit utiliser un énoncé d'avis de confidentialité et un formulaire de consentement. Nous avons mis en place des règles rigoureuses, et nous veillons à ce que les différents ministères les connaissent.

M. Ziad Aboultaif: Étant donné que toute cette initiative a été lancée à cause de la pandémie, pourriez-vous nous dire, pour que les Canadiens et aussi les décideurs des partis d'opposition aient une idée de ce que le gouvernement veut faire, à quand remonte la dernière loi ou politique présentée par votre ministère?

● (1735)

L'hon. Joyce Murray: Je vais demander à Marc Brouillard, le dirigeant principal de l'information par intérim, de vous répondre.

Le président: Monsieur Brouillard, soyez bref, je vous prie.

M. Marc Brouillard (dirigeant principal de l'information du Canada par intérim, Secrétariat du Conseil du Trésor): Veuillez m'excuser, mais vous avez bien demandé à quand remonte la dernière mise à jour de la politique en matière de protection de la vie privée?

M. Ziad Aboultaif: Oui.

M. Marc Brouillard: Je ne me souviens pas exactement, mais ça fait pas mal de temps.

Je pourrais obtenir...

Le président: Étant donné qu'il ne reste plus de temps, pourriez-vous faire parvenir à notre greffier, le plus rapidement possible, les informations précises que M. Aboultaif vous a demandées?

M. Marc Brouillard: Volontiers.

Le président: Merci beaucoup.

M. Ziad Aboultaif: Merci.

Le président: Je donne maintenant la parole à M. Weiler, pour cinq minutes.

M. Patrick Weiler (West Vancouver—Sunshine Coast—Sea to Sky Country, Lib.): Merci, monsieur le président.

Je remercie la ministre et les autres témoins de participer à notre réunion aujourd'hui.

Je salue également tous les employés qui se sont rapidement adaptés au télétravail et qui ont réussi, en peu de temps, à assurer un service de grande qualité. Par ailleurs, je trouve incroyable et rassurant qu'aucun fonctionnaire n'ait été victime d'une cyberattaque pendant la pandémie.

Madame la ministre, pouvez-vous nous dire ce que fait le gouvernement du Canada, en cette période de transition numérique, pour protéger les renseignements personnels des citoyens?

L'hon. Joyce Murray: Nous parlions justement de la protection de la vie privée et de la politique du gouvernement dans ce domaine. Tous les fonctionnaires reçoivent une formation sur cette politique et la connaissent bien.

Services partagés Canada joue un rôle très important dans la protection de la vie privée et des renseignements personnels des Canadiens, car c'est la principale organisation responsable de l'entreposage de ces renseignements. C'est en quelque sorte le gardien de la majorité de ces renseignements. Ses employés doivent respecter des directives très claires sur l'utilisation et l'entreposage des documents sécurisés, et il tient par ailleurs un inventaire de tous les renseignements personnels traités par ses employés. Services partagés Canada restreint et administre la collecte, l'utilisation, l'entreposage et la divulgation des données, conformément à l'esprit et à la lettre des lois relatives à la protection des renseignements personnels. C'est pour nous une priorité absolue.

Paul, avez-vous quelque chose à ajouter?

M. Paul Glover: Merci, madame la ministre.

J'ajouterai simplement que tous les employés qui travaillent dans les centres où sont entreposées ces données doivent avoir une habilitation de sécurité. Tous les centres de données sont surveillés. Les données sont codées, et, par conséquent, même si nous voulions les regarder, nous ne pourrions pas les déchiffrer. Il faut connaître les clés, au départ et à l'arrivée, et ce sont donc les ministères qui reçoivent les données qui peuvent les utiliser de façon appropriée. Nous prenons cette précaution pour être sûrs que tous ceux qui utilisent ces données ont l'habilitation de sécurité appropriée. Comme les données sont toujours codées, elles ne sont accessibles qu'à ceux qui ont besoin de les voir.

M. Patrick Weiler: Je vous remercie de votre réponse.

J'aimerais maintenant savoir ce que fait le gouvernement en matière de cybersécurité, notamment ce qu'il fait pour contrer des cybermenaces ciblant des infrastructures gouvernementales ou, éventuellement, des entreprises privées?

L'hon. Joyce Murray: Dans le domaine de la cybersécurité, nous avons adopté une approche très intégrée pour ne pas avoir des systèmes disparates au sein d'un même gouvernement. C'est grâce à cela que nous connaissons les succès dont nous vous avons parlé aujourd'hui en ce qui concerne la diminution des vulnérabilités et des intrusions. C'est le Centre canadien pour la cybersécurité qui a la responsabilité de s'assurer que les réseaux et activités gouvernementaux ne sont pas ciblés par des piratages ou des menaces.

Cette approche coordonnée est pilotée par un triumvirat composé du bureau du dirigeant principal de l'information, de Services partagés Canada et du Centre de la sécurité des télécommunications. C'est ce triumvirat qui a élaboré ce qu'on appelle le Plan de gestion des événements de cybersécurité du gouvernement du Canada, de sorte que dès qu'un événement ou un incident se produit, chacun sait précisément qui doit faire quoi, ce qui renforce l'efficacité de toute l'organisation.

Je vais demander à Scott s'il a quelque chose à ajouter.

● (1740)

Le président: Monsieur, vous avez environ 30 secondes pour répondre.

M. Scott Jones: Merci. J'ai simplement quelques précisions à ajouter.

Nous utilisons les multiples niveaux de défense qui existent au gouvernement du Canada. Ensuite, nous mettons à la disposition des entreprises canadiennes ce que nous avons appris en défendant le gouvernement du Canada.

Nous le faisons de toutes sortes de façons. Par exemple, nous transmettons ces renseignements à l'Autorité canadienne pour les enregistrements Internet, afin que tous les Canadiens puissent profiter de ce qu'on appelle le Bouclier canadien, dont je pourrais vous parler si vous le voulez. Nous pouvons aussi décider d'envoyer des indicateurs uniques de tentatives d'intrusion qui n'ont encore jamais été révélés à personne ailleurs dans le monde, parce que nous avons réussi à construire un système de défense hors-pair pour le gouvernement. Nous essayons d'en faire profiter tous les Canadiens, y compris, bien sûr, les entreprises canadiennes.

Le président: Merci beaucoup.

Je redonne la parole à M. Aboultaif, pour cinq minutes.

M. Ziad Aboultaif: Le comité des opérations gouvernementales a demandé une fois au ministère… Le ministère du Gouvernement numérique a indiqué que 11 % du portefeuille d'applications du gouvernement fédéral est inutilisé.

Madame la ministre, pouvez-vous nous donner des chiffres précis sur le nombre d'applications qui ne sont pas utilisées ou, plutôt, qui n'ont pas été évaluées?

L'hon. Joyce Murray: Puis-je vous demander, monsieur Aboultaif, à quelles fins elles seraient évaluées?

M. Ziad Aboultaif: Pour tout, leur validité, leurs avantages, leur utilité.

Vous savez comme moi qu'un grand nombre de centres numériques ont été fermés ou ne sont toujours pas utilisés. Nous en avons déjà parlé. Je me demande donc, en ce qui concerne les applications logicielles, combien n'ont pas encore été évaluées.

L'hon. Joyce Murray: Je vous remercie de votre question.

Les applications logicielles appartiennent aux ministères qui les utilisent pour assurer la prestation de leurs services. Ces applications ne relèvent pas du ministère du Gouvernement numérique.

Il y a beaucoup d'applications logicielles, environ 18 000, dont certaines sont d'anciennes applications. C'est un fait. Nous encourageons tous les ministères à réduire le nombre d'applications qu'ils utilisent et à les consolider, et nous les encourageons aussi à suivre des principes numériques, pour que nous ayons tous la même approche et que nous puissions nous échanger des applications.

M. Ziad Aboultaif: Voulez-vous dire que les 18 000 applications n'ont pas été évaluées, c'est bien cela?

L'hon. Joyce Murray: Je vais demander à M. Brouillard de vous répondre.

M. Marc Brouillard: Merci, madame la ministre.

Le chiffre de 18 000 représente le nombre total d'applications qui se trouvent dans notre portefeuille d'applications. Pour un certain nombre d'entre elles, les ministères se livrent chaque année à un exercice d'évaluation de leur statut, de leur fiabilité et, comme vous l'avez dit, de leur validité technique. Sur la totalité de cet inventaire, il y en a à peu près 10 ou 11 % qui ne font pas l'objet d'une évaluation, soit parce qu'elles ont été fermées, soit parce qu'on a oublié d'en faire une.

Mais inversement, nous avons plus de 90 % des applications qui font l'objet d'une évaluation.

M. Ziad Aboultaif: Dans sa réponse, le ministère indique que 7 363 applications logicielles n'ont pas été évaluées. C'est ce que dit le rapport préparé par votre ministère. En fait, pour employer les mots exacts, le ministère indique que 7 363 applications logicielles n'ont pas été validées.

Puisque seulement 36 % des applications sont fiables et que les autres ne le sont pas, peut-on en conclure que l'infrastructure numérique est en train de s'effondrer?

L'hon. Joyce Murray: Je vous remercie de votre question.

Je dirai qu'au Canada, nous sommes en train de restructurer nos fondations technologiques d'Internet et des télécommunications afin de mieux servir les Canadiens. Dans bien des cas, ça marche, mais je reconnais qu'il y a des systèmes, des centres de données et des applications qui sont anciens et qui posent des problèmes, et nous nous employons à y remédier petit à petit.

● (1745)

M. Ziad Aboultaif: Comme je l'ai déjà mentionné, 36 % des applications sont en bon état. L'autre 64 % ne l'est pas, c'est-à-dire les deux tiers.

Quel échéancier vous êtes-vous donné, madame la ministre, pour assurer le bon état de fonctionnement de 100 % de nos applications?

Le président: Vous avez 30 secondes, madame la ministre.

L'hon. Joyce Murray: Je vais demander à M. Brouillard de répondre.

M. Marc Brouillard: Merci, madame la ministre.

L'important n'est pas... Nous n'avons pas fixé d'échéancier pour l'ensemble des applications. Nous devons nous concentrer sur la modernisation des applications qui sont vraiment essentielles et qui ont la plus grande valeur opérationnelle pour le gouvernement, et c'est ce que nous faisons. Le plan consiste à répertorier ces applications et à les transférer vers des centres de données à l'état final ou le nuage.

Le président: Merci beaucoup.

Nous en sommes à la dernière ronde de questions de cinq minutes

Monsieur Kusmierczyk, vous avez cinq minutes.

M. Irek Kusmierczyk (Windsor—Tecumseh, Lib.): Merci, monsieur le président.

Je vais poursuivre dans la même veine que mon collègue. D'après le Plan ministériel 2020-2021 de SPC, près de 80 % des quelque 18 000 applications du gouvernement sont hébergées dans des centres de données vieillissants et peu fiables qui sont plus susceptibles de pannes de service et de défaillances, et le ministère accordera la priorité au déplacement de ces applications vers le nuage ou des centres de stockage de données d'entreprises.

La pandémie de COVID-19 a-t-elle accéléré ce processus et la migration vers le nuage présente-t-elle des avantages sur le plan de la cybersécurité? Je pense que je vais m'arrêter à ces deux questions pour l'instant.

L'hon. Joyce Murray: Oui, la migration vers le nuage présente des avantages, c'est certain. La sécurité est un des grands avantages, et l'optimisation des coûts en est un autre.

Je vais demander à Paul Glover, de Services partagés Canada, de nous dire si le processus de migration vers les centres de données, dans lequel notre gouvernement a investi il y a quelques années et qui est sur la bonne voie, s'est poursuivi même si nous avons dû recentrer nos efforts sur les demandes urgentes et tout à fait inattendues de millions de Canadiens.

M. Paul Glover: Merci, madame la ministre.

Je peux vous assurer que nous avons continué ce travail. Il est très important. Certains édifices arrivaient à la fin de leur vie utile. Il fallait déménager les centres de données qui s'y trouvaient vers ce que nous appelons des centres de données à l'état final, de conception plus moderne. Nous continuons de travailler très fort. Au cours des deux dernières années, nous avons dépassé nos objectifs et atteint des taux de 120 % l'année dernière et de plus de 100 % cette année. Une centaine de centres de données ont été fermés depuis un an.

Les fermetures restent beaucoup moins nombreuses, mais notre but n'est pas seulement de fermer des centres de données. Comme vous l'avez souligné, notre travail doit être centré sur les applications qui sont stockées dans ces centres et sur la mise au point de stratégies efficaces pour les maintenir en état de fonctionnement. C'est exactement ce que nous faisons. Nous les déplaçons vers des centres de données plus modernes. Quand c'est impossible, nous remplaçons le matériel pour éliminer les risques. Il n'est pas toujours nécessaire de déplacer les applications. Dans certains cas, un bon travail de maintenance et de mise à niveau peut suffire pour rendre une application fonctionnelle.

Pour ce qui concerne le nuage, le processus s'est effectivement accéléré parce que la vitesse et la taille sont devenues des enjeux majeurs. Il a été question tout à l'heure des centres d'appels qui traitaient quelques milliers d'appels et qui tout à coup doivent en traiter des centaines de milliers à la minute. Il a fallu augmenter la capacité très rapidement, et c'est ce que le nuage permet de faire.

Nous sommes ravis de pouvoir compter sur la collaboration du CST et les orientations stratégiques du DPI pour assurer une migration vers le nuage en toute sécurité tant pour la population canadienne que pour le gouvernement. Nous avons un canal sécurisé vers le nuage, ce qui signifie que le réseau et le chemin d'accès aux applications stockées dans le nuage sont protégés.

Tous nos contrats de services infonuagiques sont protégés. Par exemple, pour ce qui concerne la Patriot Act et d'autres mesures du genre, les centres de données dans les nuages doivent être en sol canadien pour que les ministères puissent y entreposer des renseignements protégés. Le travail s'est intensifié, et nous nous assurons qu'il s'effectue dans un cadre très sûr et très sécuritaire.

● (1750)

M. Irek Kusmierczyk: Merci pour cette réponse très détaillée.

Dans le même ordre d'idées, le gouvernement fédéral a-t-il été l'objet d'un moins grand nombre d'incidents de cybersécurité touchant ses applications déjà stockées dans le nuage?

M. Paul Glover: Je vais répéter ce que Scott Jones a dit tout à l'heure. Notre périmètre est vraiment de calibre mondial et il fait l'envie de bien des pays. Il intercepte la grande majorité des menaces, alors de dire qu'il n'existe aucun... Les menaces se comptent par milliards tous les jours, mais elles sont neutralisées. Et dans les très, très rares cas où elles atteignent leur cible, elles sont repérées très rapidement et réprimées. Les services sont interrompus, mis hors connexion et débranchés avant qu'il y ait des dommages. À ma connaissance, aucun incident n'a menacé la sécurité des données au cours des 10 dernières semaines. Des incidents sont interceptés tous les jours, mais ils n'ont jamais de conséquences graves.

L'hon. Joyce Murray: Si vous me le permettez, j'aimerais ajouter...

Le président: Je vous demanderais d'être très brève, madame la ministre.

L'hon. Joyce Murray: D'accord.

J'aimerais informer le public qui nous écoute ou qui nous regarde, de même que les députés, qu'ils peuvent télécharger gratuitement le coupe-feu Bouclier canadien de l'ACEI. Il peut être utilisé par les petites entreprises et par tous les Canadiens. Ce coupe-feu est le fruit de l'expérience et de l'expertise de l'équipe de collaborateurs issus des différentes initiatives de cybersécurité du gouvernement canadien.

Le président: Merci infiniment.

Nous allons maintenant passer à des rondes de questions de deux minutes et demie. Nous commencerons avec M. Barsalou-Duval.

[*Français*]

M. Xavier Barsalou-Duval (Pierre-Boucher—Les Patriotes—Verchères, BQ): Je vous remercie beaucoup, monsieur le président.

Tout à l'heure, j'ai entendu à répétition que, depuis le début de la pandémie de la COVID-19 où l'on a incité davantage les gens à travailler de la maison, il n'y avait eu aucun problème de sécurité, aucune intrusion ni aucune fuite de données concernant nos fonctionnaires. Ce serait aussi le cas, semble-t-il, pour le personnel de la Chambre des communes.

Cependant, j'ai aussi entendu que, dans la majorité des cas où il y a des fuites, des fuites de données ou de l'espionnage, par exemple, les gens n'en sont pas conscients ou ne le remarquent pas.

Comment savez-vous qu'il n'y en a eu aucune, alors que les gens s'en rendent rarement compte?

[*Traduction*]

L'hon. Joyce Murray: Merci de soulever cette question.

Tout d'abord, je peux vous garantir que notre priorité absolue a été de maintenir les services à la population canadienne et de fournir aux fonctionnaires les outils requis pour offrir ces services à l'intérieur du périmètre de sécurité du gouvernement canadien. Et nous avons réussi.

Nous avons aussi indiqué clairement quelles activités requièrent d'utiliser les circuits sécurisés et lesquelles peuvent être menées sur des plateformes publiques comme Zoom. Je vais demander à M. Glover d'expliquer comment nous...

[*Français*]

M. Xavier Barsalou-Duval: Vous ne pouvez donc pas me garantir qu'il n'y a pas eu de fuites, de fuites de données, d'espionnage ni de quoi que ce soit d'autre.

[*Traduction*]

M. Paul Glover: Scott pourra compléter ma réponse pour ce qui concerne le CST, mais je peux vous dire que nous le savons parce que nos outils de surveillance du trafic nous permettent de comprendre... Ce sont des outils intelligents, qui utilisent l'intelligence artificielle et d'autres dispositifs — les coupe-feu — pour intercepter les menaces et surveiller ce qui se passe. S'il y a une tentative de redirection du trafic qui a été marquée comme inappropriée, nous allons la détecter et la bloquer.

Monsieur Jones.

Le président: Monsieur Jones, je sais que vous resterez avec nous pour la prochaine heure. Vous pourrez peut-être compléter la réponse plus tard, mais nous n'avons vraiment plus de temps. Je suis désolé.

Nous passons à la dernière ronde.

Monsieur Green, vous avez deux minutes et demie. Nous vous écoutons.

M. Matthew Green: Merci, monsieur le président.

Dans son Plan stratégique des opérations numériques de 2018 à 2022, le gouvernement fédéral reconnaît la nécessité de moderniser l'infrastructure et les systèmes de TI vieillissants. Il indique aussi qu'il y a un risque que les biens et les systèmes de TI qui ont atteint la fin de leur cycle de vie utile ne respectent pas les exigences actuelles et émergentes en matière de prestation de services et de renseignements essentiels en temps opportun à la population canadienne.

Madame la ministre, dans votre lettre de mandat, le premier ministre vous a demandé de recenser tous les systèmes et toutes les plateformes de TI qui sont de base et à risque. Le gouvernement fédéral a-t-il modernisé son infrastructure et ses systèmes à risque depuis le début de la pandémie? Si c'est le cas, quel est le coût estimatif de la mise à niveau de tous les systèmes et de toutes les plateformes de TI qui ont été jugés de base et à risque?

● (1755)

L'hon. Joyce Murray: Merci.

Vous venez de décrire une tâche assez monumentale. Il faudra des années pour la réaliser. Services partagés Canada a reçu 2,2 milliards de dollars dans le budget de 2018, et d'autres crédits ont été annoncés depuis.

Je vais demander à M. Brouillard, le dirigeant principal de l'information par intérim, de vous donner plus de détails.

M. Marc Brouillard: Merci, madame la ministre.

Comme vous l'avez mentionné, le budget de 2018 prévoyait des fonds pour cette modernisation, y compris une affectation de 110 millions de dollars pour la modernisation des applications qui visait à soutenir la migration des applications anciennes des ministères vers des infrastructures infonuagiques modernes. Par la même occasion, les ministères peuvent faire un examen de leurs procédés numériques et chercher des moyens d'améliorer la prestation des services.

Le recensement des services de base est en cours. Les systèmes essentiels qui doivent être modernisés ont été répertoriés, et nous continuons d'offrir notre collaboration et notre soutien aux ministères pour ces initiatives.

M. Matthew Green: Merci, monsieur le président.

Le président: Un grand merci à vous tous.

Madame la ministre, notre première période de questions se termine ici. Nous vous remercions sincèrement d'avoir participé à la séance d'aujourd'hui. Je ne crois pas me tromper en affirmant que quand vous avez accepté de devenir ministre du Gouvernement numérique, vous n'aviez aucune idée, et nous non plus d'ailleurs, que nous nous retrouverions dans un monde aussi virtuel et que vous et vos fonctionnaires auriez une telle responsabilité. Merci d'avoir été des nôtres. Nous vous en sommes très reconnaissants. Je vous souhaite bonne chance, et j'espère que vous resterez en santé et en sécurité.

L'hon. Joyce Murray: Merci.

Le président: Si vous le voulez bien, chers collègues, nous allons poursuivre sans faire de pause, mais je vais tout de même laisser le temps à la ministre de se retirer.

Nous passerons directement à la deuxième heure, au cours de laquelle nous nous entretiendrons avec le dirigeant principal du Centre de la sécurité des télécommunications, M. Scott Jones. Il va nous présenter une brève allocution d'ouverture de cinq minutes.

Monsieur Jones, nous vous écoutons.

M. Scott Jones: Merci, monsieur le président. Merci de m'avoir invité à venir discuter avec vous aujourd'hui.

Je suis le dirigeant principal du Centre canadien pour la cybersécurité, lequel relève du Centre de la sécurité des télécommunications, ou CST. Le CST est l'un des principaux organismes de renseignement du Canada, ainsi que l'autorité technique et l'organisme d'opérations du Canada en matière de cybersécurité. Nous relevons du ministre de la Défense nationale.

Le CST continue de tirer parti de tous les moyens dont il dispose en vertu de son mandat pour veiller à ce que le Canada soit protégé contre les cybermenaces et à ce que le gouvernement du Canada ait accès aux renseignements qui permettront d'alimenter les processus décisionnels visant les approches à préconiser face à la COVID-19.

Créé en octobre 2018, le Centre pour la cybersécurité est une source unifiée de conseils et d'avis d'experts, de services et de soutien visant les enjeux opérationnels du domaine de la cybersécurité. En outre, il constitue, pour les citoyens canadiens et les entreprises du Canada, une source transparente et fiable de conseils sur tout ce qui touche à la cybersécurité. La pandémie de COVID-19 nous a obligés à adapter notre routine quotidienne et a une incidence sur notre façon de travailler et de communiquer.

En cette période d'incertitude, les auteurs malveillants tentent de tirer parti du niveau élevé d'inquiétude ressenti par les Canadiens à l'égard de la COVID-19. À juste titre, bon nombre de Canadiens sont devenus craintifs et tendus, et cette réaction émotionnelle peut être exploitée en ligne. Nous avons d'ailleurs constaté un accroissement du nombre de cas où des auteurs malveillants se servent de la COVID-19 pour mener des campagnes d'hameçonnage et de fraude par maliciels.

Je me propose de faire le point sur le travail que le Centre pour la cybersécurité accomplit pour protéger les Canadiens, les systèmes essentiels, la Chambre des Communes et le gouvernement du Canada contre les actes de cyberfraude commis avant, pendant et après la pandémie.

Tout d'abord, le CST continue de tirer parti de tous les moyens dont il dispose en vertu de son mandat pour veiller à ce que le Canada soit protégé contre les menaces. Le Centre pour la cybersécurité met tout en œuvre pour sensibiliser le public aux risques liés aux cybermenaces qui pèsent sur les organismes de santé canadiens, et ce, en adoptant une approche préventive consistant, notamment, à publier des alertes sur les cybermenaces, et à prodiguer des conseils et des consignes préparés sur mesure pour les organismes de santé canadiens, les partenaires gouvernementaux et les partenaires de l'industrie.

En plus de prodiguer des conseils et des consignes aux organisations canadiennes, nous misons de plus en plus sur Pensez cybersécurité, la campagne de sensibilisation du public, pour aider les Canadiens à appliquer eux-mêmes les mesures qui leur permettront de protéger leurs activités en ligne. De concert avec les partenaires de l'industrie et les membres du réseau international des organismes de cybersécurité, le Centre pour la cybersécurité a largement contribué à l'élimination de sites Web frauduleux et d'autres mécanismes employés pour appâter les Canadiens, notamment des sites affichant frauduleusement les couleurs du gouvernement du Canada, comme je l'ai mentionné tout à l'heure.

En effet, un nombre important de travailleurs et d'organismes se sont tournés vers le télétravail et l'apprentissage en ligne en raison de la pandémie de COVID-19. Par conséquent, les appareils et les dispositifs employés pour effectuer les tâches requises sont devenus des cibles prisées par les auteurs de cybermenaces. Les auteurs de cyberattaques cherchent désormais à exploiter les connexions établies pour le télétravail, étant donné que les télétravailleurs exécutent leurs tâches à l'extérieur du périmètre sécurisé normalement fourni par leur employeur et que la transition a dû se faire rapidement.

En l'occurrence, le Centre pour la cybersécurité s'est associé à l'Autorité canadienne pour les enregistrements Internet, l'ACEI, dans le but de créer et de mettre en place le Bouclier canadien de l'ACEI. La ministre a très bien expliqué ce que fait l'ACEI, et j'aimerais profiter de l'occasion pour la remercier de son leadership remarquable en mettant au service des Canadiens un mécanisme de protection des activités en ligne. L'ACEI est un partenaire inestimable pour nous.

Pour renforcer la protection des Canadiens, nous avons pris une autre mesure essentielle qui consiste à les tenir au courant des enjeux de cybersécurité. Grâce à la publication de conseils et de consignes spécialement conçus, le Centre pour la cybersécurité permet de renforcer la protection des ressources électroniques des Canadiens. Nous avons partagé des conseils de sécurité sur les outils de vidéoconférence et de téléconférence, et sur le télétravail en général pour informer et éduquer les Canadiens et les aider à prendre des décisions éclairées en ce qui concerne la sécurité en ligne.

Le Centre pour la cybersécurité a créé tout un éventail de conseils et de consignes, dont plusieurs sont devenus plus pertinents que jamais. D'ailleurs, j'encourage les Canadiens à visiter notre site Web pour en apprendre davantage sur les directives et les pratiques exemplaires qu'il convient de mettre en pratique pour se protéger.

Pour soutenir les programmes gouvernementaux d'importance, nous avons assuré une surveillance de tous les instants, par exemple la soumission en ligne des demandes de Prestation canadienne d'urgence, dont M. Glover a parlé plus tôt.

De plus, depuis un certain temps, nous évaluons les applications infonuagiques, notamment pour l'Agence de la santé publique du Canada, et nous avons activé une fonction de surveillance et de cyberdéfense visant toute forme d'utilisation des nuages dans l'ensemble du gouvernement canadien. Le Centre pour la cybersécurité a continué de collaborer avec le Centre antifraude du Canada, qui relève de la GRC, la Police provinciale de l'Ontario et le Bureau de la concurrence du Canada, des organismes qui constituent des sources canadiennes sûres et fiables lorsqu'il s'agit de signaler et d'atténuer l'effet des fraudes par marketing de masse.

Je suis également heureux de mentionner que le Centre pour la cybersécurité travaille en partenariat avec la Chambre des Communes depuis plusieurs années. Maintenant que le Parlement s'est tourné vers les réunions virtuelles, le Centre pour la cybersécurité collabore avec la Chambre des Communes afin de lui offrir des conseils et des avis sur mesure, et notamment en soutien aux assemblées virtuelles et aux réunions des comités. Les conseils et les avis prodigués par le Centre pour la cybersécurité ont aidé la Chambre des Communes à prendre des décisions éclairées en ce qui concerne le choix, l'installation et l'utilisation des outils de vidéoconférence et de téléconférence. Nous sommes très fiers de soutenir les efforts déployés pour assurer la continuation des débats parlementaires.

En dernier lieu, il importe de noter que le gouvernement du Canada entretient des relations privilégiées avec ses partenaires internationaux de la cybersécurité. En l'occurrence, nous échangeons régulièrement des renseignements, ce qui a des répercussions positives importantes sur le maintien de la sûreté et de la sécurité de nos pays respectifs. Je tiens à rassurer les Canadiens sur le fait que le CST et le Centre pour la cybersécurité travaillent sans relâche pour atténuer les menaces et les protéger.

Merci de votre attention.

● (1800)

Le président: Merci, monsieur Jones.

Nous allons amorcer les rondes de questions de six minutes, en commençant par M. McCauley.

M. Kelly McCauley (Edmonton-Ouest, PCC): Merci, monsieur le président.

Monsieur Brouillard, je vous souhaite la bienvenue. Mes premières questions s'adresseront à vous et porteront surtout sur l'accès à l'information.

Est-ce que nous avons actualisé les directives données aux employés en matière de gestion de l'information au sein du gouvernement du Canada?

M. Marc Brouillard: Vous voulez dire pour ce qui concerne les nouvelles conditions de travail, le travail à...

M. Kelly McCauley: Oui, bien évidemment.

M. Marc Brouillard: Nous avons rappelé à tous les fonctionnaires fédéraux qu'il leur incombe, à l'égard de toute information à valeur opérationnelle qui est stockée dans un appareil du gouvernement du Canada qui est utilisé à domicile, de s'assurer qu'il n'y a aucun risque...

M. Kelly McCauley: Oui, mais faisons-nous autre chose que leur rappeler les directives existantes?

M. Marc Brouillard: Nous leur rappelons que c'est leur responsabilité et qu'ils peuvent utiliser les infrastructures publiques comme Zoom ou d'autres sites de collaboration seulement pour du matériel non classifié.

M. Kelly McCauley: D'accord.

La directive sur la tenue de dossiers propose des pratiques efficaces pour la gestion et la protection de l'intégrité de l'information des ministères.

Étant donné que beaucoup de fonctionnaires travaillent maintenant à domicile, pouvez-vous me dire quelles modifications ont été apportées premièrement pour protéger l'information, et deuxièmement pour en assurer l'accès si jamais elle fait l'objet d'une demande d'accès à l'information?

M. Marc Brouillard: Nous avons recommandé de maintenir l'accès aux réseaux et à tous les outils nécessaires pour les fonctionnaires fédéraux qui fournissent des services essentiels. À ceux qui ne fournissent pas de services essentiels et à qui nous pouvons demander de se connecter aux réseaux après les heures normales de travail ou de manière intermittente, nous rappelons qu'ils ont toujours la responsabilité de retourner les dossiers à valeur opérationnelle dans les systèmes.

Un certain délai peut être toléré parce qu'il n'est pas toujours possible de se connecter au réseau. Cela dit, les fonctionnaires travaillent à la maison avec du matériel sécurisé fourni par le gouvernement, et ils ont toujours accès au réseau.

M. Kelly McCauley: Bien.

Le processus de demande d'accès à l'information a été suspendu. Nous savons que les fonctionnaires travaillent de la maison. Quand est-il prévu de reprendre les activités pour que le public, les politiciens et tous ceux qui le souhaitent puissent recevoir une réponse à leurs demandes d'accès à l'information?

M. Marc Brouillard: Je ne crois pas que le processus a été complètement suspendu.

Là encore...

M. Kelly McCauley: Oui, il est complètement suspendu.

M. Marc Brouillard: Il est complètement suspendu?

M. Kelly McCauley: Je vous mets au défi de trouver une seule réponse donnée depuis deux mois.

M. Marc Brouillard: Je vais devoir m'informer.

Bien entendu, il faut comprendre que les fonctionnaires n'ont pas accès à leur bureau et qu'ils ne sont peut-être pas en mesure de faire le même type de recherches qu'ils feraient normalement en interne...

● (1805)

M. Kelly McCauley: Est-ce que vous avez un plan pour régler le problème? Nous ne pouvons pas rester les bras croisés et accepter l'idée que le processus d'accès reste suspendu indéfiniment. Est-ce qu'un plan est envisagé ou allons-nous rester sans rien faire et attendre de voir ce qui arrivera avec la pandémie?

M. Marc Brouillard: Nous collaborons avec le Bureau du dirigeant principal des ressources humaines pour planifier la reprise des activités et le retour au travail. Nous nous attendons à des arriérés dans certains secteurs d'activités, et notamment dans le traitement des demandes d'accès à l'information, et ils seront considérés comme des priorités. Cette planification est en cours.

M. Kelly McCauley: La commissaire à l'information, Mme Maynard, s'est montrée très critique, pour le dire poliment, de la manière dont le gouvernement traite actuellement son devoir de transparence. Sur son site Web, elle a publié un message dans lequel elle rappelle aux institutions qu'elles doivent continuer de fournir la documentation justificative de leurs décisions et de leurs processus décisionnels, ainsi que l'exige la Politique sur la gestion de l'information.

Comment nous assurons-nous que cette exigence est remplie autrement que par une mention concernant l'utilisation des serveurs du gouvernement?

M. Marc Brouillard: Cette politique s'adresse aux ministères. L'application de la politique relève des ministères, et c'est eux qui doivent s'assurer que les documents essentiels pour justifier les décisions...

M. Kelly McCauley: La fonction de surveillance incombe au DPI du Conseil du Trésor. Encore un exemple où on nous dit que c'est la responsabilité des ministères et que c'est bien dommage s'ils ne s'en acquittent pas, mais que peut-on y faire?

M. Marc Brouillard: Je ne dirais pas que c'est dommage. Je pense néanmoins qu'il incombe aux ministères et à leurs administrateurs de faire appliquer les politiques du Conseil du Trésor.

M. Kelly McCauley: Oui, d'accord, mais quel genre de suivi le Conseil du Trésor peut-il faire pour vérifier s'ils le font? C'est ce qui m'intéresse.

M. Marc Brouillard: Je comprends.

En fait, nous faisons une surveillance continue de la conformité et nous faisons des rapports annuels, pour rendre compte au...

M. Kelly McCauley: Comptez-vous intensifier la surveillance continue considérant que le processus d'accès à l'information est au point mort et qu'il y a vraiment matière à s'inquiéter si nous nous fions à la mise en garde de la commissaire à l'information?

M. Marc Brouillard: Pour le moment, nous concentrons nos énergies à comprendre comment nous pouvons soutenir les ministères et à renforcer leur capacité, en mettant l'accent sur les priorités opérationnelles.

M. Kelly McCauley: Dans quelle mesure êtes-vous certain que la Politique sur la gestion de l'information sera appliquée?

M. Marc Brouillard: Je dirais que j'en suis assez certain parce que tout le monde réalise à quel point c'est important. La collaboration et la communication n'ont jamais été aussi fortes dans la communauté, nous savons tous de quoi il s'agit et il existe une réelle volonté de la faire appliquer.

M. Kelly McCauley: Merci.

J'aurais une dernière question sur le même sujet. Sur son site Web, la commissaire donne neuf conseils sur la gestion de l'information transmise par courriel. Avez-vous communiqué ces conseils aux ministères ou allez-vous attendre qu'ils en prennent connaissance par eux-mêmes sur le site Web?

Là encore, c'est la responsabilité du Conseil du Trésor. Si vous laissez faire, et nous en avons eu de nombreux exemples, que ce soit dans les dossiers des ressources humaines, des dénonciateurs ou des plans ministériels... C'est sa responsabilité, mais il préfère la déléguer aux ministères et on n'aboutit à rien.

M. Marc Brouillard: Je n'ai pas personnellement...

Le président: Monsieur Brouillard, je vais vous demander de transmettre votre réponse par écrit au greffier, comme je l'ai mentionné plus tôt, dès que possible. Je n'ai aucun doute que vous voulez donner une réponse détaillée à M. McCauley, et je vous donne la possibilité de le faire le plus rapidement possible.

Nous passons maintenant à la ronde suivante de questions, qui durera six minutes également.

Monsieur Jowhari.

M. Majid Jowhari (Richmond Hill, Lib.): Merci, monsieur le président.

Bienvenue à tous nos témoins. Je tiens à vous remercier pour les éclairages que vous nous avez donnés jusqu'ici.

Ma question s'adresse à M. Brouillard. Plusieurs de mes collègues ont posé des questions sur un aspect précis que j'appelle les piliers ou les pierres d'assise de notre stratégie numérique ou de notre gouvernement numérique, que ce soit la cybersécurité, l'infrastructure vieillissante, etc. Pour la gouverne des nombreux Canadiens qui nous regardent, pourriez-vous revenir un peu en arrière et nous expliquer en quelques mots les quatre ou cinq piliers de la stratégie numérique du gouvernement?

Où en étions-nous dans la réalisation de notre mandat avant la pandémie de COVID-19, et quelles répercussions a eu cette pandémie sur notre mandat et sur notre capacité à le réaliser? Je vous poserai d'autres questions sur le même sujet ensuite.

M. Marc Brouillard: Je ne suis pas certain de comprendre. Vous me demandez d'expliquer comment, en contexte de COVID-19, la stratégie numérique...

M. Majid Jowhari: Avant la pandémie de COVID-19, un mandat a été donné. La ministre a reçu une lettre de mandat. En tant que DPI, pourriez-vous nous dire ce qui selon vous constitue la pierre d'assise de la stratégie numérique de notre gouvernement?

● (1810)

M. Marc Brouillard: D'accord. La réponse est un peu complexe, mais je vais tenter de la décomposer.

Le gouvernement canadien regroupe diverses composantes et il reste du travail à faire dans chacune de ces composantes. Paul Glover pourra sûrement vous en dire davantage à ce sujet mais, pour ce qui concerne la modernisation de l'infrastructure afin de répondre aux besoins en matière de connexion dans notre monde interconnecté... Nos réseaux doivent être efficaces et capables de communiquer entre eux. La cybersécurité, qui est le sujet de la réunion, représente un impératif stratégique absolu. Nous devons garder en lieu sûr et traiter convenablement les renseignements que nous confient les Canadiens.

La gestion de l'information, je le répète, vise à protéger les renseignements personnels des Canadiens, mais elle vise aussi à soutenir les initiatives de gouvernement ouvert pour qu'ils puissent avoir accès à toute l'information à laquelle ils ont droit.

Ensuite, pour ce qui concerne les applications et la prestation des services, nous devons nous assurer d'utiliser des méthodes modernes de développement et de conception, en tenant compte des normes et des principes numériques, qui mettent toujours l'utilisateur au premier plan. Si les services ne sont pas conçus en fonction des utilisateurs finaux, qu'il s'agisse de particuliers ou d'entreprises canadiennes...

M. Majid Jowhari: Excellent. C'est exactement la réponse que j'espérais. Je voulais entendre vos explications sur les différentes pierres d'assise.

Puis arriva la COVID-19. De toute évidence, elle a eu des répercussions sur la stratégie, ou sur la feuille de route si vous préférez, que nous nous étions engagés à suivre. Pouvez-vous nous dire en quelques mots quel a été l'effet général de la pandémie sur notre capacité à mettre en oeuvre cette stratégie? Quel aspect a été le plus touché?

M. Marc Brouillard: Services partagés a relevé l'énorme défi de revoir la configuration complète du réseau, qui était centrée sur les employés dans les lieux de travail qui communiquent avec l'extérieur, mais qu'il a fallu transformer parce que beaucoup de personnes travaillent maintenant chez elles et doivent communiquer avec leur lieu de travail. La ministre et M. Glover ont parlé un peu de ce qui a été fait. C'est le premier grand changement.

Le deuxième, clairement, a été la création de prestations pour les Canadiens. L'ARC et EDSC ont redoublé d'efforts pour assurer la mise en oeuvre de la PCU, des subventions salariales et d'autres mesures qui étaient...

M. Majid Jowhari: Je suis désolé de devoir vous interrompre. En quelques mots, quelles seront nos vulnérabilités par rapport à notre stratégie initiale?

M. Marc Brouillard: Je ne suis pas certain de comprendre. Vous voulez parler des vulnérabilités par rapport à...

M. Majid Jowhari: Je parle de ce qu'il faudra faire concernant notre capacité à réaliser notre mandat après la COVID-19.

M. Marc Brouillard: D'accord. Je ne parlerais pas de vulnérabilité, mais plutôt de changement...

M. Majid Jowhari: C'est une zone à risque.

M. Marc Brouillard: C'est aussi un changement de priorités, qui est tout à fait justifié. Je crois que les raisons de ce changement sont valables. Quand nous amorcerons la planification de la reprise des activités et du retour au travail dans les bureaux, nous ramènerons à l'avant-plan les priorités que nous avons établies avant la pandémie. Ce sera l'étape suivante.

M. Majid Jowhari: Pouvez-vous me donner un exemple de priorité à laquelle il faudra porter une attention particulière quand nous accélérerons la reprise et ouvrirons l'économie?

M. Marc Brouillard: Ce n'est pas vraiment mon champ d'expertise. Je m'occupe davantage des opérations internes du gouvernement.

M. Majid Jowhari: Oui, je comprends, mais les opérations internes du gouvernement soutiennent ces initiatives.

M. Marc Brouillard: Oui, absolument. Nous veillons à ce que les ministères responsables disposent de toute l'infrastructure requise pour fournir leurs services. C'est l'une de nos grandes priorités et c'est au coeur de notre travail.

M. Majid Jowhari: Il me reste 30 secondes. Est-ce que nous avons les ressources en capital, les fonds nécessaires pour atteindre nos objectifs? Si nous ne les avons pas, sur quoi devrions-nous nous concentrer pour les trouver?

Le président: Je vous demanderais de répondre très brièvement.

M. Marc Brouillard: La réponse brève est que cela devra faire partie de notre réflexion au cours du processus de planification et d'établissement des priorités.

M. Majid Jowhari: Merci.

Le président: Merci beaucoup.

[*Français*]

Madame Vignola, vous avez la parole pour six minutes.

Mme Julie Vignola: Excusez-moi. L'interprétation a été coupée, alors je n'ai pas tout entendu.

Dans le plan ministériel, Services partagés Canada a fait remarquer que les menaces informatiques étaient constantes. Tout à l'heure, on parlait de 2 milliards d'attaques quotidiennes contre différents services gouvernementaux. C'est du moins ce que j'ai entendu.

Premièrement, de quelles ressources Services partagés Canada dispose-t-il pour prévenir ces attaques?

Deuxièmement, existe-t-il une collaboration avec les autres services policiers, notamment la SQ?

Troisièmement, d'où viennent ces attaques? Viennent-elles de sources internes, au Canada, ou des sources externes?

J'arrête à trois questions. Je verrai pour le reste.

Mes questions s'adressent soit à M. Brouillard, soit à M. Jones.

● (1815)

[*Traduction*]

M. Scott Jones: Je vais commencer par les questions générales sur la cybersécurité, si vous me le permettez.

Tout d'abord, pour ce qui est de la provenance, les menaces peuvent venir de partout dans le monde. C'est une caractéristique des auteurs malveillants. Ils ne sont pas tous au même endroit.

Nous nous intéressons plutôt aux moyens de nous protéger contre toutes les activités malveillantes que contre leurs auteurs. Nous collaborons avec nos collègues des services policiers. Nous travaillons avec tous les corps policiers du pays, y compris la Sûreté du Québec, de même qu'avec nos partenaires de la GRC, pour trouver des solutions.

Avant tout, nous laissons les policiers faire leur travail et nous faisons ce qui nous est demandé, qui consiste à faire de notre mieux pour améliorer la sécurité des Canadiens. Nous leur donnons des conseils sur la manière d'assurer leur propre protection, en espérant que nos collègues des forces de l'ordre... Nous essayons de recueillir le plus d'information possible pour aider les policiers à attraper les criminels responsables de la cyberactivité malveillante.

Monsieur Glover.

M. Paul Glover: Merci, monsieur Jones.

La réponse à la question sur les besoins en ressources de Services partagés comporte plusieurs éléments. Par exemple, nous avons besoin de l'expertise d'organismes comme le Centre canadien pour la cybersécurité, qui assure une surveillance continue de ces phénomènes. Nous avons aussi besoin de la technologie des réseaux et des centres de données.

Une foule d'éléments interreliés contribue à cette mission, et j'inclus même la disposition matérielle des édifices. Beaucoup de menaces viennent de l'intérieur. Par exemple, pour les centres de données, nous nous assurons toujours que les entrées et les sorties des personnes sont bien consignées dans un registre. Il faut aussi faire un contrôle très serré et très exhaustif des permissions de sortir du matériel.

Bref, c'est un travail qui comporte plusieurs volets. Notre analyse des menaces couvre tous les angles possibles. Nous nous référons beaucoup aux politiques, aux orientations et à l'expertise de nos collègues des autres organismes, et nous suivons des pratiques exemplaires pour les transposer à tous les systèmes, qu'ils soient installés dans un ordinateur de travail, un réseau ou un centre de données à l'état final, et à toutes les étapes du processus.

[*Français*]

Mme Julie Vignola: Plus tôt, on a parlé des applications. Il y en a une panoplie et des rumeurs circulent. Des entreprises voudraient avoir des applications pour surveiller leurs employés, par exemple pour calculer le nombre de clics, les sites qu'ils ont consultés, et le reste.

Le gouvernement du Canada utilise-t-il actuellement ce genre d'application pour ses propres employés qui font du télétravail?

[*Traduction*]

M. Paul Glover: Je vais tenter de répondre à la question de la députée.

Nous ne surveillons pas le temps passé en ligne. C'est la responsabilité des ministères. Nous surveillons le type de trafic, ou sa nature si vous préférez, du point de vue de la sécurité, pour nous assurer que les sites consultés sont appropriés. Nous surveillons la nature des activités à un niveau très dépersonnalisé. Souvent, la surveillance n'est pas faite par une personne, mais par un coupe-feu, par des applications d'intelligence artificielle, ce genre de dispositifs.

C'est différent de ce que font les entreprises qui veulent savoir combien de temps leurs employés passent en ligne et ce qu'ils font. La sécurité est notre seule... Nous surveillons la nature des communications, des échanges, pour nous assurer qu'il n'y a pas eu d'atteinte ou de menace.

[*Français*]

Mme Julie Vignola: Je vous remercie.

On a parlé, entre autres, d'une bande passante augmentée, de nouveaux ordinateurs, de nouvelles structures, de micros et de cybersécurité. Jusqu'à maintenant, quel est l'impact de ces nouveaux besoins sur les budgets?

● (1820)

[*Traduction*]

Le président: Vous avez environ 30 secondes pour répondre, si c'est possible.

M. Paul Glover: Oui, pas de problème.

C'est environ 58 millions de dollars au total. C'est ce qu'ont coûté les tablettes et le matériel fournis pour le télétravail, les mises à niveau des réseaux, l'ajout de points d'accès à distance protégé, les dispositifs et le matériel spécialisés pour traiter les volumes de demandes de nouvelles prestations soumises par les Canadiens. Ces volumes sans précédent ont fait augmenter les coûts de stockage et les dépenses informatiques. C'est ce qui a été investi d'un bout à l'autre de la chaîne.

Le président: Merci beaucoup.

Je vais maintenant donner la parole à M. Green. Vous avez six minutes.

M. Matthew Green: Merci.

Nous avons rarement l'occasion de poser des questions à un représentant du Centre de la sécurité des télécommunications, alors je vais en profiter pour interroger M. Jones par votre entremise, monsieur le président.

En 2018, le gouvernement fédéral a lancé le Centre pour la cybersécurité au sein du CST, en regroupant les compétences en cybersécurité du CST, du ministère de la Sécurité publique et de SPC. Combien d'employés travaillent-ils pour le Centre?

M. Scott Jones: Merci de poser cette question.

Actuellement, nous avons un effectif de 800 employés environ pour réaliser le mandat traditionnel du CST, axé sur la cryptographie, auquel se sont ajoutés des mandats de centre des opérations de sécurité du gouvernement du Canada et de CERT national.

M. Matthew Green: Combien de ces employés sont-ils issus respectivement de Sécurité publique et de Services partagés Canada?

M. Scott Jones: En tout, environ 150 employés ont été mutés.

M. Matthew Green: Et comment la sélection a-t-elle été faite?

M. Scott Jones: Certains employés exécutaient leurs fonctions actuelles au sein de leur ancien ministère. Les deux ministères ont muté des employés et nous les avons intégrés dans la structure du tout nouveau Centre pour la cybersécurité.

M. Matthew Green: Merci.

Selon un reportage des médias, le CST travaille en coordination avec ses partenaires pour faire en sorte que les sites d'hameçonnage reliés à la COVID-19 qui imitent ceux du gouvernement du Canada soient éliminés. Quels sont ces partenaires?

M. Scott Jones: Nous travaillons avec des partenaires de la communauté mondiale de la cybersécurité. Quand nous repérons des activités malveillantes qui visent notre pays, nous pouvons demander l'aide de l'équipe nationale d'intervention d'urgence en sécurité informatique, ou CERT, d'un autre pays. Nous avons aussi des contrats avec des partenaires commerciaux. Dans la mesure du possible, nous ne donnons pas le nom de nos partenaires parce que nous ne soutenons aucune entreprise en particulier. Nous avons des liens contractuels avec certaines entreprises, mais nous faisons très attention qu'elles ne nous utilisent pas pour rehausser leur image et leur réputation.

M. Matthew Green: C'était très clair. Merci.

Pourriez-vous donner d'autres exemples du travail du CST en matière de cybersécurité dans le contexte de la COVID-19?

M. Scott Jones: Oui, avec plaisir.

J'ai déjà mentionné l'élimination de sites Web frauduleux et notre collaboration avec des partenaires pour ce travail. Nous avons aussi publié de nombreuses alertes pour prévenir les organismes du secteur de la santé. Je citerai également les tables multisectorielles et notre collaboration avec diverses industries canadiennes pour discuter de la pandémie de la COVID-19 et de notre réponse. Nous avons notamment coopéré avec les secteurs des communications, de la technologie et de la santé, de même qu'avec nos partenaires des provinces et des territoires pour nous assurer de partager un maximum d'information.

Je dirais que nous avons réussi à obtenir le concours de tous les secteurs des infrastructures essentielles. Au plus fort de la crise, quand tout s'est mis à trembler et que tout le monde était sur les dents, nous recevions énormément d'appels toutes les semaines et nous transmettions constamment de l'information.

M. Matthew Green: Ma prochaine question peut paraître frivole, mais je vais quand même vous la poser parce que tout ce qui concerne les fraudes m'inquiète particulièrement. Existe-t-il de nouvelles technologies pour dépister les bons vieux stratagèmes d'hameçonnage par téléphone? Je suis député et je continue de recevoir des appels de l'ARC à mon numéro du gouvernement, dans lesquels on m'annonce que je vais aller en prison si je ne verse pas immédiatement telle somme.

Existe-t-il des moyens de lutter contre ce type de stratagème téléphonique traditionnel?

M. Scott Jones: Je reçois aussi ce genre d'appels.

M. Matthew Green: Ce doit être intéressant. Leur dites-vous pour qui vous travaillez?

M. Scott Jones: Parfois, si j'ai du temps, j'essaie de les tenir occupés en me disant que le temps qu'ils passent avec moi pourra épargner d'autres Canadiens. Ma réponse générale serait que c'est ce genre de problèmes que le CRTC et d'autres partenaires du domaine des télécommunications cherchent à régler. Malheureusement, le réseau téléphonique international est encore régi par des normes établies en 1975 dans certains cas. La sécurité du réseau ne faisait pas partie des priorités à cette époque. Ces normes ont été conçues pour quelques exploitants de réseaux téléphoniques qui étaient en situation de monopole et dont la fiabilité n'était pas mise en question, et on essaie de s'y adapter. C'est notre défi actuellement.

Nous essayons de les soutenir et de collaborer avec eux par l'intermédiaire de nos tables multisectorielles mais, à cause des conditions actuelles, le défi est de taille.

● (1825)

M. Matthew Green: Merci.

Voilà qui met fin à mes questions. Je ne vais pas continuer pour le simple plaisir d'utiliser du temps, monsieur le président.

Le président: Merci beaucoup, monsieur Green.

Nous allons maintenant entamer une série de questions de cinq minutes, et commencer avec Mme Block.

Mme Kelly Block (Sentier Carlton—Eagle Creek, PCC): Merci beaucoup, monsieur le président.

Je remercie également les témoins de leur présence avec nous aujourd'hui.

Comme vous l'avez indiqué dans votre déclaration préliminaire, monsieur Jones, nous vivons à une époque extraordinaire. Une époque qui nous force en effet à changer notre façon de travailler et de communiquer. Même si nous avons relevé le défi, je pense qu'il est plus important que jamais de sécuriser l'infrastructure essentielle maintenant que les activités gouvernementales opèrent un virage vers le numérique et le télétravail.

Vous avez également mentionné dans votre exposé, monsieur Jones, que le gouvernement du Canada entretient des relations étroites et utiles avec ses partenaires internationaux de la cybersécurité. Vous avez dit que nous échangeons régulièrement des renseignements, et que cela a des répercussions positives importantes sur le maintien de la sûreté et de la sécurité « de nos pays respectifs ». Peut-être que cette phrase enchaîne un peu sur la réponse que vous venez de faire à mon collègue, M. Green.

D'après un article paru samedi dans le *Telegraph*, le premier ministre du Royaume-Uni a annoncé son intention de réduire l'importance de la participation de Huawei dans les réseaux 5G du pays dans la foulée de l'éclosion du coronavirus. Si Huawei fait partie des réseaux 5G du Canada, est-ce que cela risque de poser un risque pour la sécurité des Canadiens?

M. Scott Jones: Il est important de mentionner qu'en ce moment même le ministre de la Sécurité publique mène un examen continu de la sécurité. Évidemment, dans le cadre de cet examen, nous apportons notre soutien relativement aux éléments liés à la cybersécurité, et nous prenons en considération tous les renseignements dont nous disposons. Trouver le moyen de sécuriser n'importe quel réseau est l'un des défis que nous devons affronter actuellement. Un concept vraiment important consiste à ne faire confiance à aucun des équipements que nous utilisons, quel qu'il soit. C'est la même approche que nous avons adoptée avec le gouvernement du Canada, en nous efforçant de superposer de nombreuses couches de défense. Il faut toujours partir du principe que dans l'éventualité où l'une des couches échouerait à assurer la protection souhaitée, une autre couche viendra prendre le relais. C'est de cette manière que nous nous dotons d'une mesure de précaution supplémentaire ou de freins et contrepoids, selon la manière dont on souhaite la décrire, afin de pouvoir mettre en place une infrastructure de sécurité multicouches.

Et ensuite, en dernier ressort, certaines autres décisions devront être prises dans le cadre de la politique.

Mme Kelly Block: Merci.

D'autres partenaires du Groupe des 5 ont déjà pris une décision concernant Huawei et les réseaux 5G. Est-ce que le contexte est différent au Canada pour que nous n'ayons pas encore pris de décision à ce sujet?

M. Scott Jones: Nous étudions cette question afin de pouvoir formuler des conseils en matière de cybersécurité dans le cadre de l'examen à plus grande échelle qui est en cours. L'un des principaux aspects à considérer, en ce qui nous concerne, consiste à tirer parti de l'expérience que nous avons acquise depuis 2013 en exécutant un programme d'examen de la cybersécurité. Ce programme consistait à améliorer la sécurité avec nos partenaires de télécommunications dès le départ. Nous nous efforçons de tabler sur cette expérience qui permet de fournir au gouvernement une source de renseignements déterminants et rigoureux pour prendre ses décisions.

Mme Kelly Block: Selon vous, serait-il même possible pour le Canada de prendre une décision dès maintenant concernant la participation de Huawei à nos réseaux 5G?

M. Scott Jones: Les normes relatives aux réseaux 5G évoluent constamment. L'un des facteurs clés en ce qui nous concerne consiste à s'assurer que peu importe le fournisseur — c'est-à-dire, peu importe le pays d'origine du fournisseur — nous construisons un protocole de sécurité qui est indifférent à l'origine. La chaîne d'approvisionnement est compliquée pour tous les fournisseurs, et l'une des priorités en ce qui nous concerne est de faire en sorte que le Canada soit protégé, sans égard au fournisseur, quel que soit le lieu où se trouvent les Canadiens, et de nous assurer de mettre en place ces relations et ces éléments de sécurité d'entrée de jeu.

Mme Kelly Block: Je comprends ce que vous voulez dire lorsque vous dites considérer qu'un réseau est toujours vulnérable.

Est-ce que Huawei est considéré comme un fournisseur à risque plus élevé lorsqu'il s'agit d'un réseau 5G?

M. Scott Jones: Parmi les aspects que nous examinons toujours, il y a la manière dont les produits sont construits, l'endroit où ils sont construits, le mode d'assemblage, l'origine des composants, la propriété des entreprises, etc. Il en va de même pour tous les produits.

Nous appliquons cette expertise dans le cadre d'un concept dont nous avons déjà parlé aujourd'hui: l'intégrité de la chaîne d'approvisionnement. Cette expertise s'applique à cet égard aussi. Nous ajoutons des activités supplémentaires en matière d'atténuation, de réduction des risques, selon ces différents facteurs, afin d'essayer de réduire le risque à un niveau acceptable.

L'un des aspects les plus prenants de mon travail est que je ne peux jamais vraiment bien dormir la nuit parce qu'il subsiste toujours un risque quelque part. Le seul moyen de réduire vraiment ce risque à zéro sur Internet et dans les communications consisterait à tout débrancher. Naturellement, ce n'est pas une option envisageable.

● (1830)

Le président: Merci beaucoup.

Nous allons maintenant céder la parole à M. Drouin, pour cinq minutes, je vous en prie.

M. Francis Drouin (Glengarry—Prescott—Russell, Lib.): Merci, monsieur le président. Par votre intermédiaire, j'aimerais poser mes questions à M. Glover.

Je me rappelle, il y a près de 10 ans de cela, en 2013 je pense, il était question de Marissa Mayer, et toute la discussion tournait autour de la possibilité de faire du télétravail ou pas... Cette ancienne présidente-directrice générale de Yahoo avait déclaré, « Je ramène tous les employés au bureau, et plus personne ne travaillera à partir de la maison. »

Dans notre cas, je sais que certains employés pouvaient travailler de la maison, mais aujourd'hui, la COVID-19 a frappé et tout le monde doit faire du télétravail. Pourriez-vous me parler de cette possibilité d'améliorer la capacité d'autoriser le télétravail, et de permettre aux fonctionnaires de travailler depuis la maison?

M. Paul Glover: Absolument, avec plaisir. Toutes mes excuses si je gruge le temps qui vous est alloué; vous n'avez qu'à me faire signe, et je m'arrêterai.

Nous avons énormément travaillé en ce sens. Ce fut vraiment sans précédent. Nous avons commencé par ce que nous appelons les points d'accès à distance protégé, afin de procéder en toute sécurité.

Lorsque M. Jones a parlé de tout le travail accompli à cause de la COVID, l'une des choses qu'il a omis de vous dire c'est tous les conseils qui nous ont été donnés afin que nous procédions de manière sécuritaire. Cela consistait notamment à établir des points d'accès à distance protégé pour que les fonctionnaires puissent travailler de façon sécuritaire.

Nous avons travaillé avec toutes les grandes entreprises de télécommunications et tous les fournisseurs Internet afin d'augmenter l'étendue de la bande passante, et de la spécialiser dans les endroits où nous savions qu'elle était fragile. Nous avons travaillé avec les premiers répondants afin de voir à ce qu'ils aient l'accès en priorité aux lignes requises. Ce furent des activités vraiment multidimensionnelles.

Nous avons réalisé très rapidement que ce n'était pas seulement le nombre de points d'accès à distance protégé qui était pertinent. Mais aussi la bande passante. Il fallait tenir compte de la manière dont ils travaillaient, des tâches qu'ils accomplissaient — et c'était vraiment varié. Nous avons dû augmenter réellement l'étendue de la bande passante. Nous avons tout simplement pratiquement doublé le nombre de points d'accès à distance protégé, et nous avons aussi pratiquement doublé l'étendue de la bande passante réservée à cet effet. Il y a eu d'énormes changements dans cet espace.

La ministre a parlé des opérateurs de centre d'appels, par exemple. Nous avons fait en sorte qu'ils disposent de tablettes et de téléphones, afin qu'ils ne soient pas forcés de se rendre dans un centre d'appels proprement dit. Nous avons travaillé avec les entreprises de télécommunications ainsi qu'avec les fournisseurs de services pour nous assurer que la technologie fonctionnait. C'est d'ailleurs en partie la raison pour laquelle, au début, nous avons échappé — très peu, franchement — quelques appels. Nous avons travaillé rapidement à trouver une solution, afin d'acheminer ces appels dans les foyers des opérateurs afin qu'ils puissent y répondre.

Nous avons aussi réalisé qu'il n'était pas nécessaire que tout le monde dispose d'un accès à distance protégé, aussi nous avons travaillé à la création de ce que nous appelons le site de collaboration du gouvernement. Il repose sur Microsoft Office 365 et Teams dans le nuage, mais il n'est pas protégé. Les fonctionnaires peuvent toujours continuer de collaborer avec leurs collègues sur une plateforme financée par le gouvernement, mais qui n'est pas protégée. Ils sont au courant. Nous allons ultérieurement démanteler ce site afin qu'aucun renseignement ne soit perdu.

Nous avons essayé de donner aux employés le plus d'outils et de choix possible pour pouvoir poursuivre nos activités. Nous avons doublé notre capacité de faire des vidéoconférences. Nous sommes en effet passé de près d'un million de minutes, un million et demie de minutes par jour de téléconférences à plus de cinq millions de minutes par jour.

Il s'agissait, littéralement, de créer une capacité. Il fallait fournir non seulement une tablette et une connexion Internet, mais aussi les téléphones correspondants, la vidéoconférence, la sécurité, le service pour stocker toutes les données relatives à la PCU et avec un nombre croissant de demandeurs. Ce fut vraiment assez exhaustif.

M. Francis Drouin: Monsieur Glover, j'ai appris d'après le site Web Achatsetventes.gc.ca, par exemple, que des services de TI et des produits de TI ont été désignés comme des priorités pour des enjeux liés à la COVID. Est-ce que votre organisation a fait appel aux mêmes fournisseurs que ceux avec lesquels vous faites affaire habituellement, ou avez-vous effectué des modifications à l'intérieur du système pour permettre... ? Peut-être qu'il existe sur le marché de nouveaux produits dont nous ignorons encore l'existence, ou des solutions intéressantes qui ont été offertes par le truchement d'Achatsetventes.

Comment votre ministère a-t-il pesé le pour et le contre et choisi entre « je vais faire affaire avec les gens que je connais » et « il se pourrait qu'il existe de nouvelles solutions dont nous n'avons pas encore entendu parler »?

● (1835)

M. Paul Glover: La réponse à la question du député comporte deux volets distincts.

Premièrement, nous devions agir rapidement. Il fallait donc jongler avec l'ampleur et la vitesse, et nous cherchions des partenaires chez les fournisseurs susceptibles de répondre à ces critères. Il fallait pouvoir fonctionner dans les circonstances qui nous occupaient — c'est-à-dire répondre aux millions de Canadiens qui allaient ouvrir une session simultanément le premier jour — nous n'avions pas droit à l'échec. Nous devions être prêts. Les systèmes devaient fonctionner, aussi nous devions collaborer avec des personnes qui pouvaient fonctionner à la vitesse et avec l'ampleur que nous cherchions. Il ne s'agissait donc pas de travailler avec des gens que nous connaissions, mais plutôt de mettre l'accent sur la vitesse, l'ampleur et la sécurité.

Étant donné que nous exerçons nos activités partout au pays, nous avons dû examiner nos relations avec les PME. Nous ne pouvions pas nous rendre partout où il aurait fallu aller. Nous avons donc modifié le modèle opérationnel pour permettre, par exemple, à des partenaires dignes de confiance de configurer et d'installer le matériel à notre place. Nous procédions à la vérification et à l'expédition directement afin d'accélérer le processus. Nous avons innové de cette manière, en essayant de faire participer un plus grand nombre de PME, surtout celles qui peut-être avaient bien besoin de trouver du travail, et il n'en manquait pas. Dans la mesure où les entreprises respectaient nos exigences en matière de sécurité, nous pouvions les intégrer à l'écosystème. Il s'agissait donc d'une équipe hybride.

Bien franchement, j'ai reçu...

Le président: Très brièvement, monsieur, vous avez dépassé le temps alloué, alors essayez de conclure au cours des 16 prochaines secondes, s'il vous plaît.

M. Paul Glover: J'ai reçu des offres concernant de nouvelles technologies pratiquement tous les jours. Nous avons travaillé avec des partenaires à l'évaluation de ces technologies afin de trouver celles qui pouvaient nous être utiles. Nous avons été littéralement inondés d'offres de nouveaux services et nous sommes encore en train de faire le tri.

Le président: Merci.

Monsieur McCauley, je vous en prie.

M. Kelly McCauley: Merci.

Monsieur Jones, j'aimerais poursuivre dans la veine de la question posée par Mme Block concernant Huawei. Vous avez déclaré que nous devons nous protéger contre tous les fournisseurs. Est-ce que vous avez la même impression au sujet des deux autres grands fournisseurs, Ericsson et Nokia, pour les serveurs, qu'envers Huawei, c'est-à-dire que nous devons faire preuve de prudence à leur endroit?

M. Scott Jones: Nous faisons en sorte d'évaluer chacun des produits et chacune des entreprises en fonction de ses caractéristiques propres; et ensuite, nous essayons diverses mesures d'atténuation, selon l'origine.

M. Kelly McCauley: Vous avez mentionné une réduction des risques supplémentaire. Diriez-vous que le risque est plus élevé avec Huawei que, disons, Ericsson ou Nokia?

M. Scott Jones: Les risques sont différents. L'un des éléments que nous recherchons est...

M. Kelly McCauley: Quels sont les risques inhérents à Huawei, disons par rapport à Ericsson?

M. Scott Jones: Par exemple, nous déterminons l'origine des produits, l'endroit où ils ont été construits, l'endroit où le logiciel a été écrit. En règle générale, pour la majorité de ce matériel, le problème ne tient pas vraiment au matériel proprement dit, mais plutôt au logiciel. De nos jours, les logiciels sont écrits à divers endroits dans le monde. L'un des facteurs que nous examinons, c'est le cadre de mise à l'essai qui les accompagne.

M. Kelly McCauley: Donc, vous placez Huawei au même niveau pour ce qui est du risque lié à la sécurité que, disons, Nokia ou Ericsson.

M. Scott Jones: Nous tiendrions compte du risque au moment d'appliquer les diverses mesures d'atténuation. Par exemple, le programme d'essais en laboratoire que nous avons mis en place avec un laboratoire canadien indépendant qui procède à des tests supplémentaires. Il s'agit là d'une mesure d'atténuation supplémentaire que nous avons mise en place pour le réseau 4G existant.

M. Kelly McCauley: Permettez-moi de vous poser deux ou trois questions. La ministre a mentionné tout à l'heure qu'il était de notoriété publique que Zoom n'est pas une plateforme protégée. Beaucoup d'employés du gouvernement utilisent Zoom. Qu'est-ce que vous pensez du fait que des réunions de caucus confidentielles — des conservateurs, des libéraux, des néo-démocrates ou des bloquistes — sont tenues à l'aide de Zoom, s'il est notoire que cette plateforme n'est pas protégée?

M. Scott Jones: Les bombardements de Zoom sont un phénomène. Nous en avons beaucoup entendu parler au début de la pandémie de la COVID. Nous pouvons faire des choses comme utiliser les salles d'attente virtuelles, comme nous l'avons fait ici, des codes et des mots de passe uniques, et communiquer ces renseignements de manière à réduire autant que possible le nombre de personnes qui peuvent...

Pour ce qui est de la communication proprement dite, nous n'avons jamais évalué la plateforme Zoom sur le plan de la protection de renseignements délicats, comme pour les communications de niveau protégé B au gouvernement.

M. Kelly McCauley: Est-ce que nous ne devrions pas le faire pourtant? Les libéraux au pouvoir tiennent leurs réunions de caucus avec Zoom, et les députés de l'opposition et du NPD discutent de renseignements gouvernementaux confidentiels.

M. Scott Jones: Nous avons travaillé avec la Chambre des communes en vue de trouver l'équilibre adéquat. Malheureusement, c'est la sécurité... Aucun produit ne possède toutes les caractéristiques dont nous avons besoin en plus des aspects liés à la sécurité que nous souhaiterions avoir, et il s'agit réellement de trouver la juste mesure entre utiliser...

M. Kelly McCauley: Quelle est la qualité de votre sommeil en rapport avec une telle question? Est-ce que vous dormez sur vos deux oreilles ou faites-vous de l'insomnie et des cauchemars en raison de l'absence de sécurité pour les députés qui utilisent le programme prescrit à la Chambre des communes?

M. Scott Jones: Je suis très à l'aise avec l'utilisation de la plateforme Zoom pour ces besoins. Je pense que la manière dont nous avons travaillé avec la Chambre des communes pour mettre ce système en place et atténuer les risques...

M. Kelly McCauley: Je ne parle pas des travaux des comités qui sont ouverts au public. Je veux plutôt parler des renseignements confidentiels, comme ceux qui sont échangés lors des réunions de caucus ou peut-être lors des réunions du Cabinet, si ces réunions se tiennent à l'aide de Zoom.

M. Scott Jones: Lorsque nous travaillons avec le personnel de la Chambre des communes, c'est notamment en vue de fournir une solution pour les réunions de caucus ainsi que pour les votes électroniques, afin d'ajouter des couches supplémentaires de sécurité. C'est une chose sur laquelle nous travaillons depuis le début, c'est-à-dire améliorer la sécurité, tout en conservant la convivialité. Nous nous efforçons de trouver un juste équilibre avec la Chambre des communes. Nous avons d'ailleurs mis sur pied une équipe qui travaille à temps plein avec la Chambre des communes pour vous appuyer.

● (1840)

M. Kelly McCauley: Dans votre exposé, vous avez mentionné que vous surveillez et protégez les programmes, dont la PCU, contre les cybermenaces. Quelle est la menace dans ce cas précis? S'agit-il de programmes en double? Est-ce que des pirates s'attaquent à la PCU? La raison pour laquelle je pose la question, c'est qu'un article publié aujourd'hui dans le *National Post* mentionne que l'on s'inquiète à l'idée que des personnes de l'étranger puissent présenter une demande. S'agit-il de s'assurer que les utilisateurs du réseau privé virtuel se trouvent réellement au Canada pour présenter une demande? Quelles sont vos inquiétudes à ce sujet?

M. Scott Jones: Nous cherchions essentiellement à repérer quiconque tenterait de se faire passer pour le gouvernement du Canada et, par exemple, mettrait sur place un site semblable à celui de la PCU en vue de tromper les Canadiens, et de les amener à croire qu'il s'agissait du site légitime de la PCU...

M. Kelly McCauley: Je cite vos paroles exactes, « contre les cybermenaces ». Il ne s'agit pas d'une cybermenace contre la PCU. Il s'agit plutôt d'une menace d'hameçonnage ou de fraude. Peut-être que votre formulation était boiteuse, ou alors, était-ce intentionnel?

M. Scott Jones: Non, il s'agit bien d'une cybermenace, parce que les fraudeurs l'utilisent dans le cadre de l'hameçonnage. Ils s'en servent pour inciter les Canadiens à révéler des renseignements personnels ou confidentiels.

Le deuxième aspect qui nous préoccupe, toutefois, c'est de nous assurer d'être prêts à réagir contre les attaques par refus de service, afin que le site demeure opérationnel et disponible pour les Canadiens. C'est un aspect sur lequel nous travaillons étroitement avec nos partenaires de Services partagés Canada.

M. Kelly McCauley: Très bien. Voici ma dernière brève question, je suis sûr...

Le président: Malheureusement, monsieur McCauley, nous n'avons plus le temps.

M. Kelly McCauley: Merci, monsieur le président.

Le président: Nous allons maintenant céder la parole à M. MacKinnon, pour cinq minutes. Je vous en prie.

[*Français*]

M. Steven MacKinnon: Bonjour à nouveau. Je tiens à vous remercier de vos efforts.

On parle beaucoup de retour au travail par les temps qui courent ainsi que des préparatifs, même si on ne connaît ni les modalités ni les dates du retour à nos bureaux. Le gouvernement du Canada a passé beaucoup de temps à revoir son modèle du bureau de l'avenir.

Ma question s'adresse principalement à M. Glover. Pourriez-vous nous en dire plus sur le côté technologique du bureau de l'avenir dans la fonction publique et dans une optique de travail de l'après-COVID-19? Je parle évidemment de la disponibilité d'Internet sans fil, d'infonuagique et d'autres outils.

[*Traduction*]

M. Paul Glover: Pour répondre brièvement à votre question, afin d'être prêt sur le plan numérique, il faut avoir des outils numériques d'accès. Cela signifie que, tout comme vous savez avant d'utiliser une prise de courant qu'elle va fonctionner, au bureau nous devons mettre en place des points d'accès câblés qui fonctionnent et il nous faut aussi des points d'accès sans fil.

Nous savons bien que ces deux choses sont de plus en plus une réalité, et que les gens se déplacent. C'est donc ce qui a été intégré à la nouvelle norme sur laquelle nous avons travaillé avec SPAC. Tous les nouveaux aménagements comportent des points d'accès câblés et sans fil afin que les employés puissent bien fonctionner. Cela nous permet aussi de nous adapter aux exigences changeantes en matière de sécurité. Et par-dessus le marché, les réseaux sont en train de changer. En effet, nous sommes en train de passer à ce que l'on appelle la « confiance zéro ». Ainsi, à tout moment, quel que soit l'appareil, nous pouvons faire en sorte que les fonctionnaires soient en mesure de travailler.

Pour fonctionner dans un environnement numérique, il faut avoir accès aux outils. Nous devons donc nous assurer que l'accès et la connectivité, tout comme l'éclairage et le chauffage, sont au rendez-vous et fonctionnels. Ils ne doivent pas être trop lents non plus, parce qu'alors, rien ne va plus. Il faut pouvoir compter sur une certaine qualité, sur la sécurité et sur la disponibilité. Ce sont ces caractéristiques qui ont été intégrées à la norme. Ce sont les critères que nous tentons d'appliquer dans tous les nouveaux milieux de travail du gouvernement fédéral. Franchement, le plus difficile, c'est la modernisation des immeubles existants plus anciens, mais la technologie s'améliore. Nous avons demandé à l'industrie de répondre au défi, et nos travaux s'accélèrent dans ce domaine également.

M. Steven MacKinnon: C'est fantastique.

Je sais que l'un des projets auxquels votre organisation a beaucoup contribué est un projet pilote appelé CotravailGC. Pour la gouverne de mes collègues, il s'agit d'un projet pilote dans le cadre duquel des employés issus de différents ministères peuvent travailler à partir d'un milieu de travail situé plus près de leur domicile ou encore, s'ils sont en déplacement, d'un milieu de travail possédant tous les outils technologiques et la sécurité nécessaires.

Pourriez-vous nous parler un peu de CotravailGC et de la facilitation technologique que vous avez apportée dans ce contexte?

● (1845)

M. Paul Glover: Essentiellement, cette question constitue un virage fondamental. Actuellement, bon nombre de personnes arrivent au travail, s'assoient au même bureau, utilisent le même téléphone. Mais ces espaces de collaboration du gouvernement du Canada sont tout le contraire. Il s'agit en effet d'un ensemble de lieux normalisés où un fonctionnaire peut se présenter, brancher sa tablette, se connecter au réseau, voir son numéro de téléphone apparaître, et se mettre à travailler. Il n'est pas nécessaire de se rendre toujours au même lieu de travail.

L'expérience d'employés qui ont déménagé dans cet espace s'est avérée exceptionnellement positive. Cet espace permet aux équipes de s'organiser elles-mêmes, de se rencontrer là où cela leur convient. Il permet aux employés de bénéficier de la possibilité de travailler plus près de la maison et de mieux concilier vie professionnelle et vie personnelle. Les commentaires des employés, alors que nous sommes à établir les plans en vue du retour au milieu de travail — parce que nous n'avons jamais réellement cessé de travailler, donc il ne s'agit pas de revenir travailler, mais plutôt de retourner dans le milieu de travail — sont que ces espaces jouent un rôle extrêmement important en leur offrant la souplesse dont ils ont besoin lorsqu'ils éprouvent des problèmes avec la garderie, l'école et ainsi de suite. Il s'agit d'un outil formidable. Je m'attends à ce que la rétroaction à l'issue de ces projets pilotes soit très positive et à ce qu'il y ait un mouvement en vue de les accélérer.

Dans ce nouvel univers, il y aura évidemment des enjeux liés à la propreté et à l'hygiène dont il faudra tenir compte afin de voir à ce que les choses se passent en toute sécurité, mais d'un strict point de vue fonctionnel, c'est le concept, c'est le modèle, et c'est la souplesse qu'il offre aux employés et aux équipes.

Le président: Merci beaucoup.

M. Steven MacKinnon: Merci.

Le président: Nous allons maintenant vers nos deux dernières interventions. Ce sont des interventions de deux minutes et demie, et nous allons commencer avec M. Barsalou-Duval.

[*Français*]

M. Xavier Barsalou-Duval: Je vous remercie, monsieur le président.

Tout à l'heure, il a été mentionné plusieurs fois que l'infonuagique était bonne pour la sécurité informatique.

Je ne suis pas un spécialiste de la sécurité informatique, mais des données ou des courriels de députés qui sont stockés sur le disque dur de leur ordinateur se retrouvent-ils finalement sur des serveurs infonuagiques de compagnies privées?

[*Traduction*]

M. Paul Glover: Monsieur le président, pour répondre à la question du député, comme il l'a mentionné, l'infonuagique se résume à un centre de données d'une taille exceptionnelle. Ce centre de données accueille souvent de nombreux locataires et donne au fournisseur la possibilité d'élargir ses possibilités. Ce qu'il y a de particulier dans la manière avec laquelle le gouvernement du Canada a abordé l'infonuagique, c'est que nous avons imposé nos exigences en matière de sécurité. Comme le disait M. Jones, les renseignements protégés B en sont un exemple. Nous exigeons notamment que l'entreprise réside au Canada. Nous exigeons le respect d'exigences sur le plan de la sécurité matérielle. Les employés de l'entreprise doivent avoir obtenu des attestations de sécurité. Lorsque nous en avons la possibilité, nous travaillons avec des partenaires en matière de sécurité qui se rendent sur place et effectuent une vérification du respect des exigences du point de vue de la sécurité.

[*Français*]

M. Xavier Barsalou-Duval: Monsieur, ma question vise à savoir si des données se retrouvent chez des fournisseurs privés. Y a-t-il une externalisation de l'infonuagique ou est-ce fait directement par le gouvernement ou des services gouvernementaux?

[*Traduction*]

M. Paul Glover: Ce sont les fournisseurs de services infonuagiques qui administrent ces centres de données. Cela comprend les données qui y sont stockées, mais encore une fois, permettez-moi d'insister sur le fait que le stockage et le chiffrement des données sont effectués en fonction des normes que nous leur imposons. Cela comprend les copies de sauvegarde, la possibilité de récupérer les données et la désignation des utilisateurs autorisés à déchiffrer ces données.

[*Français*]

M. Xavier Barsalou-Duval: Ces fournisseurs sont-ils tous canadiens ou y en a-t-il d'autres pays?

[*Traduction*]

Le président: Pourriez-vous fournir une réponse très brève s'il vous plaît.

M. Paul Glover: C'est un amalgame. Il y a de grandes multinationales, comme les services Web d'Amazon, Microsoft Azure, et des entreprises canadiennes comme ThinkOn. La clé, c'est qu'elles sont toutes tenues de respecter les mêmes exigences. Elles doivent exercer leurs activités au Canada, ainsi nous ne sommes pas assujettis à la Patriot Act par exemple. Les données résident uniquement au Canada, et nous avons parfaitement le droit de visiter les lieux, d'inspecter et de vérifier les prétentions en matière de sécurité.

● (1850)

Le président: Merci beaucoup.

Nous allons entamer notre dernière intervention de deux minutes et demie.

Si j'ai bien compris, monsieur Green, vous avez cédé votre temps à M. McCauley. Est-ce exact?

M. Matthew Green: Oui, en effet. Je souhaite vivement voir où il veut en venir avec sa question.

Le président: Merci beaucoup.

Monsieur McCauley, la dernière intervention d'une durée de deux minutes et demie vous appartient.

M. Kelly McCauley: Merci.

Monsieur Jones, j'aimerais revenir à vous, et encore une fois, à votre déclaration préliminaire dans laquelle vous avez dit, « En dernière analyse, il importe de noter que le gouvernement du Canada entretient des relations privilégiées avec ses partenaires internationaux de la cybersécurité. [...] nous échangeons régulièrement des renseignements, ce qui a des répercussions positives importantes sur le maintien de la sûreté et de la sécurité de nos pays respectifs. »

Ce qui nous ramène à Huawei. Nous sommes le seul pays du Groupe des 5 qui n'a pas banni Huawei de ses réseaux 5G ou qui n'a pas décidé de ne pas lui attribuer un rôle majeur. Quelles seront les répercussions de cette décision? Ne risque-t-on pas de se voir exclus du partage de renseignements vitaux si nous décidons d'aller de l'avant avec une entreprise comme Huawei?

M. Scott Jones: L'un des aspects que nous avons étudiés de près est le fait que nous sommes un contributeur. En raison de notre rôle de défenseur auprès du gouvernement, nous apportons une contribution considérable à l'écosystème de la cybersécurité dans le monde. Nos partenaires internationaux y accordent de l'importance. De fait, nous sommes l'un des principaux contributeurs dans un éventail de domaines, donc nous apportons une importante participation, et nous en retirons beaucoup en retour. Nous entendons tabler sur cela et sur l'expertise que nous avons acquise et continuer de forger de solides relations. Ce sont des relations...

M. Kelly McCauley: Ne risquons-nous pas d'être mis à l'écart et de ne pas recevoir de renseignements de ce genre si nous optons pour Huawei, alors que tous les autres pays ont banni Huawei pour des motifs de sécurité?

M. Scott Jones: Nous continuons de travailler avec nos partenaires. C'est un aspect dont le gouvernement tiendra compte au moment de prendre sa décision. En ce qui nous concerne, nous ne voyons aucun changement dans nos échanges.

M. Kelly McCauley: Pensez-vous qu'il s'agira d'une décision politique plutôt que d'une décision prise par votre ministère ou en fonction de renseignements fournis par votre ministère?

M. Scott Jones: Nous n'avons constaté aucun changement dans nos échanges avec nos alliés internationaux, y compris dans ce que nous échangeons avec eux en matière de cybersécurité. Et c'est une chose qui compte pour nous.

M. Kelly McCauley: Si nous options pour Huawei, vous dites être convaincu qu'il n'y aurait aucun changement dans nos échanges. Pourtant, nous avons entendu les Américains menacer de nous couper de l'échange de renseignements si nous choisissions Huawei. Est-ce que cela ne devrait pas vous préoccuper?

M. Scott Jones: Je ne peux pas faire de commentaires sur ce que d'autres pays ont déclaré. Pour notre part, nous continuons notre étroite collaboration avec nos partenaires internationaux, et cela fera partie de la décision.

M. Kelly McCauley: Je sais que vous ne pouvez pas parler pour les autres pays. Mais est-ce que cela n'est pas inquiétant pour vous, en tant que Canadien dans votre domaine, que nous puissions nous voir exclus si nous allons à l'encontre de la volonté de nos alliés et si nous décidons de choisir les serveurs de Huawei?

M. Scott Jones: Ce qui importe pour moi, c'est de toujours montrer que nous représentons une valeur sûre pour nos alliés. Avec un peu de chance, ils verront que nous possédons des renseignements vraiment particuliers en matière de cybersécurité, et que nous les partageons avec eux constamment.

Le président: Merci beaucoup.

M. Kelly McCauley: Je suis sidéré. Je suis complètement sidéré.

Le président: Merci beaucoup. J'aimerais remercier tous les témoins qui étaient présents aujourd'hui. Merci aux représentants de Services partagés Canada, du Secrétariat du Conseil du Trésor et, bien entendu, du Centre de la sécurité des télécommunications. Vos témoignages et les renseignements éclairés que vous nous avez fournis nous sont très utiles.

Je m'adresse tout particulièrement à vous, monsieur Jones. Je sais qu'à quelques reprises on a évoqué le fait que vous pourriez éprouver parfois de la difficulté à dormir la nuit, compte tenu du poste que vous occupez. J'aimerais vous signaler, monsieur, que c'est précisément pour cela que Dieu a inventé le vin rouge. Vous devriez peut-être y songer.

Chers collègues, nous nous réunirons de nouveau ce vendredi à 11 heures, heure normale de l'Est. J'espère que durant les quelques jours qui nous séparent de cette réunion vous demeurerez tous en bonne santé et en sécurité. À vendredi.

Bonne fin de soirée à tous.